Summary
Maryland Cybersecurity Council Meeting
March 17, 2017
12:30 – 2:30 pm
Senate Miller Building (West Room I)
11 Bladen Street
Annapolis, Maryland

Council Members Present or Represented
John Abeles, Charles Ames (for Acting DoIT Secretary Michael Leahy), Patrice Drago (for Delegate Ned Carey), Howard Feldman, Don Fry, Zack Fry (for OHS Director Walter Landon), Michael Greenberger, Clay House, Zenita Hurley (for Attorney General Frosh), Brian Israel, Ron Kaese, Belkis Leong-hong, Senator Susan Lee, Anthony Lisuzzo, Joseph Morales, Mark Miraglia (for Ken McCreedy), Henry Mueller, Rajan Natarajan, Sue Rogan, Senator Bryan Simonaire, Paul Tiao, Carl Whitman.

Quorum
The quorum requirement of 26 members was not met.

Staff and Contributors Attending
Howard Barr (Office of the Attorney General), Dr. John Cordiani (Contributor), Terri Hayes (Contributor), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Markus Rauschecker (Cybersecurity Program Manager, CHHS), and Dr. Greg von Lehmen (Council Staff, UMUC).

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

Mr. Fry welcomed those present and thanked the Council and its contributors on behalf of Attorney General Frosh. He made several announcements:

- New Council members. He noted that Senator Byran Simonaire fills the seat left vacant by former Senator Catherine Pugh and that Tami Howie, CEO of the Maryland Tech Council, will replace Martin Rosendale. He thanked the outgoing members for their service.

- Due date for subcommittee draft reports. The Council staff and the Attorney General's Office would like to have subcommittee drafts by April 15th and NLT May 1st. These reports will form the July 1, 2017 report on Council activities required by statute.

- The next Council meeting is June 1st. The meeting will be 10:00 am – 12:00 pm at UMUC. Details will follow in the calendar invite to the entire Council.

The next agenda item was the minutes for the October 18, 2016 meeting. Consideration and approval of the minutes will be an agenda item at the June 1st Council meeting.

Mr. Fry then turned to the subcommittee chair reports.

Mr. Charles Ames for Acting DoIT Secretary, Michael Leahy, Acting Chair, the Cyber Operations and Incident Response Subcommittee

Mr. Ames updated members present on initiatives of the Department of Information Technology.

- More resources have been devoted to improved data loss prevention across the Executive Branch. Stronger network access controls are being implemented. The Department is pushing toward a particular solution set that will provide better network monitoring. It aims to move beyond passwords in the next few years as part of improved identity management. More agencies are asking for vulnerability assessments.

- To improve its situational awareness, the Department is discussing trusted sensors with NSA and hopes to similarly approach the Defense Cyber Crime Center via the Maryland National Guard. Likewise, DoIT is working with the Guard to obtain the necessary authorities to allow the Guard's cyber units to work more closely with Maryland State government.

- The State will be a full participate in the FEMA Region III cyber exercise.

- General Singh as stood up the Maryland Cyber Center of Excellence to work on cyber education and workforce development issues. The inaugural meeting was in November of last year.

In the discussion, John Abeles asked if Maryland was considering an information exchange. Mr. Ames indicated that the State would be visiting New Jersey to look at its model but could not say whether that would be adopted by Maryland.

Michael Greenberger, Chair, Critical Infrastructure Committee.

With the legislative session in mind and as a general comment, Professor Greenberger shared his thought that there should be an educational program for legislators on cybersecurity. This would enhance their appreciation of the issues and better position them to assess the concerns of interests potentially affected by cyber-related bills.

With respect to the business of the Infrastructure Committee, Professor Greenberger offered the following updates:

- The subcommittee will partner with the Subcommittee on Community Outreach and Public Awareness on its depository project. The Critical Infrastructure Subcommittee will offer content that will help organizations be aware of cyber risks, will highlight tools to assess their risks, and will outline best practices to reduce risk.

- Relatedly. the subcommittee will be formulating recommendations that are aimed at providing organizations, especially small and medium-size ones, to perform risk assessments.

- An analysis of critical infrastructure (CI) in Maryland is underway and will identify the CI that the Council should be concerned with. The US DHS definition includes many sectors, and all may not rise to the top levels of concern in the State. This analysis will also address the interconnectedness of infrastructure.

- Information-sharing will be a new focus for the subcommittee. The members will be looking at different models and will come forward with recommendations to the Council.

In a comment, Mr. Ames underscored the critical difference information sharing can make since threats migrate from sector to sector and across state lines.

<u>Senator Susan Lee, Chair, Law, Policy and Legislation Subcommittee.</u>

Senator Lee offered a summary of where key bills emerging from her subcommittee stood in the legislature. She recognized the critical contributions of Zenita Hurley, Howard Barr and others at OAG, Paul Tiao and Howard Feldman of her subcommittee, and Professor Greenberger and Markus Raushecker at CHHS.

- The security freeze bill (SB 270/HB 212) passed both the Senate and the House with minor differences. These are expected to be ironed out in conference. Only seven states have such legislation, and passage will be a significant benefit for Maryland consumers.

- The MPIPA commercial breach bill (SB 525/HB 974) includes updates to the definition of PII, takes into account HIPPA and other federal law, and provides clarity about the time-to-notification requirement, among other changes. The Senator noted that the bill is in the Finance Committee and urged Council members so inclined to support the legislation. Senator Lee was instrumental in passing the original MPIPA legislation as she was the later Maryland state breach law.

- Still in the Senate Finance Committee, the bill requiring that the State Department of Information Technology to consider the NIST Cybersecurity Framework (SB 286) is not likely to pass this year. Senator Lee noted that the NIST framework is the result of extensive

federal government and private sector collaboration, is being widely implemented both within and outside of critical infrastructure sectors, and would be very helpful to the Department in its security efforts.

- The ransomware bill was withdrawn. There was the perception on the part of House Judiciary Committee and the Senate Judicial Proceedings Committee that the current extortion law could be applied to ransomware cases. Because ransomware is such a threat to the business community—already impacting businesses in Maryland—the bill will be proposed again next year. There will be more time to put into clear relief for legislators how the current law is insufficient and a separate statute is needed.

- The subcommittee continues to do research in developing its recommendation for the cyber first responder reserve. The questions concern its role vis-à-vis other resources in the State and how it will be organized and managed. Colonel Bratton's presentation in October about the Maryland Air Guard's cyber operations unit was very useful to the subcommittee.

Ms. Leong-hong asked Senator Lee if Maryland had laws that covered computer crimes. The Senator answered that there are but that they do not address ransomware in the way that they should. The proposed ransomware bill recognizes the gravity of such attacks by making them a felony and attaching a large fine as a deterrent.

Mr. Ames asked if Maryland law addressed email spoofing. Senator Lee indicated that there is Maryland law that is concerned with impersonation, but she was not sure whether the law could be applied to spoofing.

Ms. Leong-hong observed that committee testimony by those affected is the most powerful. She suggested approaching the healthcare industry and other entities in Maryland to testify. Senator Lee agreed and stated that she tries to do this as much as possible. In the current session, at least one ransomware victim (a small business) did provide testimony for the ransomware bill.

Mr. Kaese suggested that it might be persuasive to have prosecutors and attorneys at firms representing victims to testify about what is lacking in the law and the tools they would like to have. Mr. Lore, Senator Lee's Chief of Staff, stated that the Maryland State's Attorneys Association agreed to provide testimony in favor of the ransomware bill but that the coordinator was not able to come on the day of the hearing.

Mr. Tiao pointed out that firms that have experienced a ransomware attack are not eager to have their incident back into the public eye. For that reason, if attorneys in private practice were to provide testimony, they most likely would come from larger law firms representing many clients over a range of issues. Those attorneys could safely speak about ransomware cases without any risk of client identification.

In a comment from the public, Dr. John Cordani (a faculty member at UMUC) observed how serious the impacts of ransomware attacks can be. In the case of hospitals, locking up systems and critical information can result in death. The penalties should be high.

Senator Lee noted that life imprisonment is not provided for in the current extortion statute. Mr. Lore sketched the penalties in the current Maryland extortion law and referenced a few states across the nation that have separate ransomware laws.

Senator Lee was appreciative of the discussion and welcomed the suggestions as excellent ones.

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

Dr. von Lehmen explained that Dr. Katz was not able to participate in the meeting because of his schedule. He noted that Dr. Katz's subcommittee outlined six preliminary proposals in the July 2016 Interim Activities Report. It has spent a good part of the year assessing their potential value against the large domain of activity in cyber education and workforce development. Progress to date:

- The subcommittee identified a scholarship-for-service program based on the federal model as an initiative that merits further exploration.

- It is also interested in recommending initiatives that that would be helpful to K-12 in promoting computing and cybersecurity education. To assist the subcommittee, MSDE approved one of its staff, Ms. Pat Mikos, to serve as liaison to the subcommittee.

Belkis Leong-hong, Chair, Economic Development Subcommittee.

Ms. Leong-hong made her update very brief out of consideration for the lateness of the afternoon.

- The subcommittee has met once since the last Council meeting and is scheduled to meet in early April to start its draft for the July 2017 report.

- One bill emerging from her subcommittee was successful, namely, the extension of the tax credit for the cost of security clearances (SB 405/HB 89).

- With a view to the July report, the subcommittee has already organized itself into groups to capture the initiatives it discussed this year and those likely to become proposals in the next year. These may include mapping the Maryland cyber asset map being built through the Commerce Department to the business lifecycle and providing other incentives for investment in cyber start-ups, among others.

Sue Rogan, Chair, Public Awareness and Community Outreach Subcommittee

Ms. Rogan reminded that one of the charges of her subcommittee is create an online repository of educational information around cybersecurity for consumers and businesses. She noted that:

- The depository's principal value will be in collecting and organizing existing content.

- DoIT will host the depository. She welcomed the content that other subcommittees may want to add.

- As a strategy for making the depository engaging, her subcommittee is looking for stories from consumers and business about why following best practices is important. She asked for help in identifying business that might be willing to provide such stories.

- The depository's value will be tied to its currency. Her subcommittee will work with DoIT to create a process for handling updates so that updates can occur quickly.

Mr. Fry

There being no further discussion of the subcommittee reports, Mr. Fry:

- Announced that given the hour, subcommittee chairs could decide whether to use the allotted time on the agenda to meet with their members about their draft reports.

- Reiterated the timeline for the draft subcommittee reports and the next Council meeting date, time and location.

There being no further updates or discussion Council members were adjourned at 2:30 pm.