Minutes
Maryland Cybersecurity Council Meeting
October 16, 2018
10:00 am – 12:00 pm
College Park Marriott Hotel and Conference Center
At University of Maryland University College
Hyattsville, Maryland

Council Members Present or Represented (31/57)
Attorney General Brian Frosh (Chair), John Abeles, Dr. David Anyiwo, Calvin Bowman (for Pete Landon), Kristin Jones Bryce, Dr. Anthony Dahbura, Cyril Draffin, Judi Emmel, Howard Feldman, Dr. Frederick Ferrer (for David Engel), Professor Michael Greenberger, Teri Jo Hayes, Fred Hoover, Brian Israel, Miheer Khona, Keith Ross (for Linda Lamone), Secretary Michael Leahy, Mathew Lee, Senator Susan Lee, Belkis Leong-hong, Kenneth McCreedy, Secretary William Pallozzi, Jonathan Powell, Jonathan Prutow, Markus Rauschecker, Susan Rogan, Senator Bryan Simonaire, Russell Strickland, Steven Tiller, Pegeen Townsend, and Clarence Williams.

Staff Attending
Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), John Evans (CSO, DoIT), Tiffany Harvey (Chief Counsel, Legislative Affairs, OAG), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Linda Wilk (NSA Fellow, Maryland Department of Commerce), Dr. Greg von Lehmen (Council Staff, UMUC).

Subject Matter Expert Presenter
MaryAnn Tierney, FEMA Region III Administrator

Council Meeting

<u>Opening Remarks by the Chair</u>

The Attorney General welcomed the members to the meeting and expressed his appreciation for their attendance. He recognized John Evans, the new chief security officer for DoIT, who accompanied Secretary Leahy to the meeting.

Mr. Frosh noted that the Consumer Financial Protection Commission, a body created in 2016, appears to be moving toward a series of proposed amendments to the Maryland Personal Information Protection Act (MPIPA) in the 2019 session. Specifically, these could:

- Expand the definition of personal identifying information (PII) to include location tracking data, genetic information, and non-public personal information collected from social media.

- Reduce the timeline for reporting of a breach to no later than ten days after a business discovers a breach or is notified of a breach.
- Include means of improving notice to consumers.

He indicated that these issues will likely be topics of discussion in the 2019 session and that there will be an opportunity to dig into the Commission's proposals more deeply at the Council's January meeting.

Mr. Frosh looked ahead to the Council's next activity report, due to the General Assembly on July 1, 2019. He stated that Dr. von Lehmen would have more details about this requirement at the January Council meeting.

Before turning to other Council business and the presentation by Ms. Tierney, the Attorney General called for the minutes of the June 13, 2018, meeting. Motions to approve were made and seconded, and there being no objections, the minutes were approved.

Overview of the Council's Website (http://www.umuc.edu/mdcybersecuritycouncil)

Markus Rauschecker, Susan Rogan, and Dr. von Lehmen provided an overview of the Council's website to include, respectively, a) the repository and its content; b) suggestions to improve the repository's user experience and public visibility, and c) the website's Open Meeting Act functions.

The Attorney General observed that the website of his office had a number of links related to cybersecurity and consumer protection and asked if they could be identified on the Council's website too. Dr. von Lehmen stated that this could easily be done and would be. Addressing Ms. Rogan's comment about user experience, Senator Simonaire asked if a mechanism could be added that would permit site users to ask questions. Ms. Rogan responded that this was an excellent suggestion and one that her subcommittee would discuss with Dr. von Lehmen to see if it could be implemented.

Subcommittee Reports

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee, for both her and Mr. Blair Levin.

Senator Lee noted five areas in which the subcommittee is considering legislative proposals:

- Enhanced consumer privacy protection ala the California Consumer Protection Act (CCPA). At its October 3, 2018, meeting the subcommittee received a briefing on the CCPA by Ariel Johnson, senior counsel for Commonsense.org, a nonprofit dedicated to protecting the privacy rights of families and children. In brief, Senator Lee noted that the CCPA allows consumers to know what information is being collected about them and to whom it has been sold; to have selected information about them deleted or to bar the sale of information

altogether. The California statute prohibits discriminating on service and price against consumers exercising the rights it provides. For minors under 16 years of age, it requires that parents opt in to permit their children's data to be sold. The statute provides for a private right of action for certain types of breaches. The law applies equally to service providers, edge companies, and brick-and-mortar vendors. The state Attorney General's office is the enforcement agency.

- Safe harbor for firms implementing a recognized cybersecurity standard. The subcommittee's discussion focused on the issue of incentives for firms to adopt such standards. One option used by the State of Ohio would offer the right of affirmative defense to such firms sued in the wake of a breach. The subcommittee questioned whether this would actually dissuade plaintiff's attorney from pursuing a settlement. Better would be a presumption that a standard of care had been met in the case of firms that implement a recognized cybersecurity standard ala the federal SAFETY Act. The act provides certain liability protections for entities that have received a designation or certification from the Department of Homeland Security for the sale or provision of "qualified anti-terrorism technology" to customers.

- Legislation imposing penalties specifically related to ransomware. Senator Lee observed that she had previously proposed bills adding ransomware with specific penalties to the extortion statute. After her discussions with the chair of the Judicial Proceedings Committee, the subcommittee on Law, Policy, and Legislation is looking at two different approaches. One would involve including ransomware provisions and penalties in computer intrusion legislation. The other would adopt the approach of the State of Michigan which makes possession of ransomware, or any attempt to engage others to use ransomware, a felony, when the activity is knowing and there is intent to introduce ransomware into data or computer systems without authorization. Michigan law provides appropriate exceptions for research.

- Additions to MPIPA and new legislation address the security of Internet of Things (IoT) devices. The subcommittee is considering various changes to MPIPA, including possible recommendations of the Consumer Financial Protection Commission. The subcommittee may also recommend a bill that would require manufacturers of IoT devices to build in elementary security features akin to those required by recent California legislation (2018 SB 327).

Senator Lee commented on articles in the media on the cybersecurity implications of net neutrality. She noted that her co-chair, Mr. Levin, drew the attention of the subcommittee to the US Department of Justice suit against California in which it argues that the net neutrality issue has been preempted by federal action. Mr. Levin's concern is that the federal court could hand down a decision that is so broad that it could wipe away state laws on a wide range of cybersecurity issues. He suggested that Maryland consider weighing into the legal action on the side of California in order to protect the progress that states have made in this area.

Secretary Michael Leahy, Chair, Incident Response Subcommittee

The Department of Information Technology's (DoIT) primary focus is to implement recommendations from the Governor's Office of Homeland Security (GOHS). These were produced by a working group convened by GOHS under the Governor's executive order on cybersecurity last year.

These efforts concern the standardization of processes for security, privacy, and data governance. As the most obvious part of this effort, Mr. Evans will be charged to develop tools to enable agencies to assess the status of their security until all are part of the state enterprise system. In addition, DoIT has implemented new training so that state employees are educated about phishing and common best security practices. Secretary Leahy affirmed in response to a question from Senator Simonaire that this training is mandatory.

Professor Michael Greenberger, Chair, Critical Infrastructure Subcommittee

Professor Greenberger commended the CCPA as an apt model for Maryland and its forward-looking institutions. While the CCPA is the most complete privacy law in the US, it is less stringent than the EU's General Data Protection Regulation (GDPR) that applies to anyone, including Maryland firms, doing business within the 27-member EU. The GDPR, for example, has a three-day breach notification requirement. In light of its recent breaches, Facebook is under investigation by both Ireland (where it has servers) and the EU for violations of the GDPR.

The subcommittee continues to contribute to the repository. It supervises the currency of the database holdings and will soon turn over a list of nearly 100 carefully curated resources to be added. Looking to 2019, the subcommittee will launch an effort to gather more information from critical infrastructure (CI) representatives to inform its recommendation for CI protection and resiliency. In this connection, it will also explore new initiatives of the National Risk Management Center at DHS. Likewise, it will continue to contribute to efforts within the Council to produce a recommendation for a threat-sharing vehicle for the state.

With respect to critical infrastructure, Professor Greenberger noted that election security is of course on everyone's mind. In Maryland, there are advocacy groups that send emails and make phone calls calling for the state's system—particularly its absentee ballot system—to be tightened up. The subcommittee is generally of the view to defer to the Office of the Attorney General on these matters. But it has continued to discuss ideas that might be helpful to the state. One of these is to create an ad hoc subcommittee of subject matter experts to discuss election security issues under appropriate arrangements to get all the issues on the table and recommendations to address them. Professor Greenberger indicated that he would provide more details to the Attorney General's Office regarding ideas discussed within the subcommittee.

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

Dr. von Lehmen noted that the subcommittee has not been able to meet since the last full meeting of the Council, but that it would be reconvening in the new year.

Bel Leong-hong, Chair, Subcommittee on Economic Development

In its September meeting, the subcommittee discussed a number of initiatives, deciding in some cases to defer to other efforts within the Council or state government:

- Maryland Information Sharing and Analysis Organization (ISAO). The need for such an organization has been advanced by Ken McCreedy and other members of the Economic Development Subcommittee as well as by Professor Greenberger, Marcus Rauschecker and Clay Wilson on the Critical Infrastructure Committee. Ms. Leong-hong asked Ken McCreedy to comment on this initiative since the Department of Commerce has taken the lead on it.

  He noted that the Department is looking at the models implemented in other states. The first step in Maryland will be to identify resources about how businesses can protect themselves on the Maryland Express Website (https://businessexpress.maryland.gov/). This is an effort in conjunction with the State Department of Assessments and Taxation. To move beyond 4-1-1 functions to 9-1-1 services in cybersecurity will require investment and staffing.

  Consequently, the next step will be to identify how to get to that goal, whether a public/private entity, a state-financed entity, or a nonprofit. Mr. McCreedy recognized Linda Wilk, a NSA fellow with the Department of Commerce, for her research on this initiative, and thanked Judi Emmel and the NSA for the fellow's program.

- Tax credits to companies sponsoring cyber apprenticeships and paid internships. The Maryland Chamber of Commerce has led on the issue, supporting legislation in 2018 and will do so again in 2019. The subcommittee recommends this measure not only to support workforce development but also as a potential mechanism for starting security clearances for apprentice employees.
- Expediting Security Clearances. This is an issue of high importance to Maryland's cybersecurity business sector requiring a federal solution. There are two dimensions to the issue. One concerns the clearances of individual employees to work on federal contracts. The other is about making it easier for small businesses to get facility clearances so that they can compete for federal contracts. Ms. Leong-hong indicated that she would be part of a meeting with Congressman Ruppersberger on these issues the next day.
- Safe harbor for businesses implementing the NIST CsF or other recognized cybersecurity standards. Ms. Leong-hong pointed out that this issue is of interest to Senator Lee's subcommittee and that the Economic Development Subcommittee will defer to her subcommittee on it.

- Supporting cyber start-ups by allowing a tax credit against state payroll taxes. The members present were supportive of the concept.
- Cyber IP development. The subcommittee's concern is to find ways to accelerate new product development and to reduce time to market by start-ups. One way to do this is by incentivizing large firms to partner with start-ups to pilot their product. Ms. Leong-hong noted that having large clients makes it easier for start-ups to acquire additional VC funding. The subcommittee has discussed two options for achieving this end:
    - Amending SB 228 that passed last session to add this incentive. SB 228 changed the investment tax credit for start-ups to the investor from the first, changed the eligibility requirements for the same, and implemented a 'buy Maryland' tax credit program for eligible firms.
    - The alternative is to propose a stand-alone bill that would accomplish the same thing.

Sue Rogan, chair, Subcommittee on Public and Community Outreach

Ms. Rogan noted that her subcommittee continues to identify resources for the repository and expressed appreciation to the Critical Infrastructure Subcommittee for the partnership in this effort. She also noted the outreach, both federal and within the state, to make known the benefits of the credit reporting legislation that came out of Senator Lee's subcommittee, mandating no-fees for freezes and thaws of Maryland consumers affected by a breach.

Subject Matter Expert Presentation

The Attorney General welcomed Ms. MaryAnn Tierney, FEMA Region III Administrator, and thanked Mr. Russell Strickland, MEMA Director, for recruiting her to speak. He indicated that he would have to leave the meeting near the end of Ms. Tierney's presentation and asked Senator Lee to take the chair at that point.

Ms. Tierney expressed her appreciation for the opportunity to talk to the Council about cybersecurity. She delivered a PowerPoint presentation[1] (accompanying these minutes) that covered the following points:

- The current cybersecurity landscape
- Challenges that government officials face
- Federal and state resources that are available
- How the reporting of cybersecurity incidents works
- A construct for thinking about cybersecurity incidents
- FEMA's role

[1] Mr. Russell Strickland noted one correction to the slides in an October 26, 2018, email. Slide 16 lists the "Maryland Joint Operations Center". This should read the "Maryland Coordination and Analysis Center"

Ms. Tierney's presentation occasioned a number of comments and questions:

Dr. Ferrer noted that among the resources available in state is the Maryland Defense Force (MDF). The MDF cooperates with the Maryland National Guard but has independent expertise in cybersecurity. As an illustration of this cooperation, he noted the role that the MDF played in Vigilant Guard 2018, an exercise which included a simulated cyber attack on 911 centers and water systems during a hurricane scenario.

Ms. Leong-hong: could Ms. Tierney comment more about continuity of operations after a cyber incident?

Ms. Tierney: This should be addressed through a continuity of operations plan (COOP). Essential to the plan is identifying the mission critical functions of the enterprise and then providing the means and training to ensure their resiliency.

Dr. Anthony Dahbura: Could Ms. Tierney comment about the range of cyber scenarios that the government is hopefully imaging and exercising for, such as attacks on both coasts simultaneously?

Ms. Tierney: It is better not to focus on particular events, since it can be that the well-defined incident one prepares for is not the event one will encounter. Key to good continuity planning is a focus on the essentials—what is necessary for civil society to keep operating regardless of circumstances—and to be prepared to ensure that those needs can be met. This is how FEMA approaches its mission, including the prospect of managing the physical effects of cybersecurity events in particular.

Mary Jo Hayes: If there are cascading effects from a cyber incident, would that exponentially increase the effort required in managing the events?

Ms. Tierney: The answer is yes, just as it would be for similar effects caused by large natural disasters. FEMA experiences second- and third-order effects in many disasters. To prepare for these, it has groups that analyze the interdependencies within the nation's critical infrastructure. For example, if the grid goes down, one question is how to keep hospitals and cell towers operating beyond the capabilities of their generators. FEMA builds its preparedness with these interdependencies in mind.

Brian Israel: To focus on one scenario—the grid going down for a long period of time—have lessons been learned from the experience of Puerto Rico after the hurricane?

Ms. Tierney: The extended power outage in Puerto Rico underscored the importance of having a robust supply chain that is lubricated to move generators and other resources quickly to keep critical parts of the infrastructure functioning. This is something that FEMA has considerable experience doing. The agency is aware that other scenarios might require different strategies, and the agency tries to anticipate them in its planning.

Dr. von Lehmen: Given the various scenarios that have been described, has there been discussion in policy circles about involving the general public in large-scale disaster training exercises?

This might develop the muscle memory, so to speak, to enable the public to know what to do and what to expect from authorities.

Ms. Tierney: FEMA does provide some preparedness guidance to the general public, such as recommending that citizens have the capacity to make it through the first 72 hours of a disruptive event. But the premise of the question is a good one. The public is a tremendous resource in an emergency. FEMA sees this all the time, with neighbors helping each other in an emergency even before first responders can arrive.

There being no other questions, Senator Lee thanked Ms. Tierney for her substantive presentation and for her willingness to address questions.

Other Business and Adjournment

Ken McCreedy noted that Governor Hogan had issued a proclamation acknowledging October as cybersecurity month, asking that it be presented to the Council. Mr. McCreedy was recognized to make the presentation. He rose to read significant portions of the proclamation and gave the proclamation to the chair, who expressed her appreciation on behalf of the Council.

Mr. Dwight Thomas suggested that the Council invite a future speaker to address new DFARS that concern the security requirements that must be met by companies doing business with DoD. These new regulations are important given the number of firms in Maryland that are DoD contractors. The chair thanked Mr. Thomas for the suggestion.

There being no further business, Senator Lee adjourned the Council at 11:53 am.