Minutes
Maryland Cybersecurity Council Meeting
January 17, 2019
1:00 pm – 2:00 pm
East I/II
Miller Senate Office Building
11 Bladen Street
Annapolis, Maryland

Council Members Present or Represented (29/57)
Attorney General Brian Frosh (Chair), John Abeles, Dr. David Anyiwo, Calvin Bowman (for Walter Landon), Kara Contino (for Senator Bryan Simonaire), Brian Corbett, Patrice Drago (for Delegate Ned Carey), Judi Emmel, John Evans (for Secretary Michael Leahy), Brigadier General Flash (for Major General Singh), Patrick Feehan, Dr. Frederick Ferrer (for David Engel), Teri Jo Hayes, Fred Hoover, Clay House, Brian Israel, Dr. Anupam Joshi, Dr. Kevin Kornegay, Mathew Lee, Joseph Morales, Senator Susan Lee, Belkis Leong-hong, Kenneth McCreedy, Jonathan Powell, Jonathan Prutow, Rajan Natarajan, Markus Rauschecker, Susan Rogan, Russell Strickland.

Staff Attending
Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), Hannibal Kemerer (Director, Legislative Affairs, OAG), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Richard Trumka (Assistant Attorney General, Consumer Protection Division, OAG), Dr. Greg von Lehmen (Council Staff, UMUC), Steve Wengel-Sakamoto (Consumer Protection Counsel, OAG).

Council Meeting

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

The Attorney General thanked members for staying on after the reception and welcomed:
- Markus Rauschecker in his new role as chair of the Critical Infrastructure Subcommittee. He expressed appreciation for Professor Greenberger's service as chair and his willingness to continue on the subcommittee in a non-chair role.
- Hannibal Kemerer, the new Director of Legislative Affairs. He noted that Tiffany Harvey joined the new PG County Executive as chief of staff and thanked her for her service at OAG and her work with the Council.

He called for the minutes of the October 16, 2018 Council meeting, which were unanimously approved.

He asked Mr. Strickland if he wished to comment on the background documents he had shared in connection with MaryAnn Tierney's presentation on October 16. These had been distributed in advance of this meeting. Mr. Strickland shared that the documents were referenced in her presentation and that he provided them to answer any questions the members may have had.

Brief to the Council on the Personal Information Protection amendments (PIPA) recommended by the Consumer Finance Commission.

The Attorney General asked Mr. Richard Trumka to brief the Council on the amendments to MPIPA Section 14-3501. In his brief, Mr. Trumka detailed the following changes:

Section 14-3501 (f). Adds activity-tracking data, genetic information, and nonpublic social media to the definition of personal information.

Section 14-3503. Clarifies that those who maintain the data for another must meet the same standard of care as those who own or license the data.

Section 14-3504.

- Ensures that the manner in which personal information is held does not affect the duties under the law. A breach is not only a loss of "computerized" data but also includes the theft of paper records, for example.
- Reduces the notification period to the consumer to no later than ten (10) days after the discovery of the breach.
- Reduces the notice of a third-party vendor to the owner or licensee of the data to no later than three (3) days.
- In cases where law enforcement may have asked that consumer notice be delayed, the PIPA amendments would require that notice be provided within one (1) day after the hold is lifted.
- Requires direct as well as general notice to the consumer in all breaches.
- Stipulates that the breach notice to the Office of the Attorney General must include number of Maryland residents affected, how the breach occurred and vulnerabilities that were exploited, the steps taken or planned to address the breach, and a copy of the consumer notice to be provided.

Mr. Trumka noted that the shorter notice periods are consistent with the New York financial regulations and the GDPR. Stating the reporting requirements for notice to the Attorney General's Office would remedy the uncertainty that exists under the current law about what information must be submitted.

The presentation prompted a number of questions and comments from the Council:
Bel Leong-hong. In the case of breach affecting a third-party vendor maintaining the date, is the three days allowed for notice too long? Response: Mr. Trumka observed that the closer one is to discovery the less one knows about a breach, creating the likelihood of over-reporting. Twelve to

24 hours is certainly too short. The law has to allow enough time so that the security team involved can assess what happened.
Clay House. When you go through a breach investigation in a large, complicated organization, it can be very difficult to pin down exactly what happened and what the exposure is. The facts unfold slowly and are often revised as the investigation unfolds. To really know what happened and to provide notice within ten (10) days of discovery is likely to be very challenging for larger firms. Response: Mr. Trumka noted that the PIPA leaves intact the current law which permits delayed notice when necessary to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.
Clay House. To clarify then, the intent is that once an organization has the subjective reasonable understanding, the reasonable belief that data has been compromised, and the scope and the nature and the degree of the compromise, that's when the ten-day timeline would start? Response: Mr. Trumka confirmed that understanding. He observed that the change in the timeline from the current 45 days to ten days is to obtain earlier notice to consumers where practicable.

The Attorney General asked if anyone on the Council would have objections to expressing support as a body for the amendments just briefed? Mr. Bowman asked if it would be possible to send the PIPA bill around to the Council so that members could have time to read it and send any objections by email. The Attorney General agreed with the proposal and directed Dr. von Lehmen to distribute PIPA for this purpose.

Subcommittee Report-outs

Senator Lee, co-chair of the Law, Policy and Legislation Subcommittee

Senator Lee noted four areas in which legislation keyed in some measure to Council recommendations would be forthcoming:

Ransomware. Modeled on a Michigan law, the bill would make the knowing possession of ransomware with intent to use a misdemeanor with the penalty to include imprisonment or a fine or both. The length of imprisonment and the amount of the fine are keyed to the level of financial loss. The bill will provide for a research exception.

Internet of Things. The bill is modeled after the California law that just passed this summer. The bill directs manufacturers of internet of things devices that are sold in Maryland to either preprogram passwords that are unique to each connected device or have some sort of processor that requires a user to generate new means of authentication before the user is granted access to the connected device for the first time. The bill provides that the Maryland Attorney General may seek relief against a manufacturer that violates a law with a fine of $1000 for each connected device that does not have a reasonable security feature as required by the law. The cap is $100,000 for violations arising from a single model of a connected device. The bill provides

that data on violations must be shared with the Council so that it can take these violations into account in developing policy recommendations as part of its statutory mission.

Data harvesting and privacy. The Council has supported the concept of additional data privacy provisions in Maryland's law. However, California's Consumer Privacy Act has been a game changer. The Senator stated that Maryland consumers should not be left out of protections that California consumers now have. To ease business concerns about a patchwork of requirements across the nation, a bill is being drafted for the Maryland 2019 session that would align as much as possible with the protections and thresholds in the California law.

Senator Lee closed by mentioning a constitutional amendment on privacy that may be proposed in this session. She noted that ten other states have passed such an amendment.

John Evans, for Secretary Leahy, Chair of the Incident Response Subcommittee

Mr. Evans referenced the Council's past concern about DoIT implementing security policies that were compliant with recognized industry standards (NIST, FISMA, FIPS). He announced that DoIT has produced an updated draft of its security policies that do reference recognized standards. This draft has been informed by consultation with GOHS and cyber working groups across the state agencies. The draft is now in legal review.

When the guidance is finalized, Mr. Evans stated that the rollout will include DoIT outreach to state agencies to offer help a) with assessing their security status against the new guidance and b) with formulating steps to remediate areas of need. The approach will be a phased one, identifying the low hanging fruit first and how to improve in those areas. He noted that DoIT does not have the budget at this point to fund the remediation, the cost of which will have to be supported by the agencies themselves.

In addition to the new security guidance and the outreach campaign, Mr. Evans also reported that there are a number of other initiatives underway that DoIT is aggressively pursuing. One of these concerns endpoint security within DoIT itself. He noted that the goal he had establish was to raise 97% of DoIT's endpoints to a secure standard by the end of 2019. He announced that this milestone has been substantially achieved, with 96% of DoIT's endpoints raised to a secure standard by the end of 2018.

Based on his experience as a department head. the Attorney General observed that the new security guidance and help in remediation is much needed across state government. Mr. McCreedy asked if the assessment tools would be available to nonexecutive branch agencies. Mr. Evans answered that DoIT would be willing to meet with interested agencies and to offer as much assistance as his department can.

Markus Rauschecker, Chair, Critical Infrastructure Subcommittee

Mr. Rauschecker updated the Council on new resources that his subcommittee compiled for the Council's repository. These will double the number of culled and tagged resources to more than 200. He emphasized that while critical infrastructure owners are its principal constituency, the repository can in fact serve a variety of stakeholders interested in how to improve their security, including small and medium-size businesses of any kind. He recognized members of the subcommittee for their help in compiling the new submissions and especially recognized Mr. Adam McCormick, a legal intern at CHHS, who did the major share of the work.

Mr. Rauschecker also noted that the subcommittee will continue to discuss information models for the state. It is of course aware of the discussions involving DoIT and other state agencies in this connection that have been supported by the research of Linda Wilk and will seek to contribute to that effort.

He concluded by stating that members of the subcommittee stand ready to support legislative initiatives concerning critical infrastructure that would be beneficial to the state.

Dr. von Lehmen for Dr. Jonathan Katz, chair of the Education and Workforce Development Subcommittee

Dr. von Lehmen conveyed Dr. Katz's regrets for being unable to join the meeting. Dr. Katz asked that a statement be placed in the record recognizing that the State of Virginia currently has plans to invest at least $25M in university research and education in cybersecurity, including development of a campus in Northern Virginia for Virginia Tech, and that Maryland risks losing faculty, students, and businesses to Northern Virginia.

Dr. Joshi commented that the investment is actually a much broader. Virginia Tech is receiving about a $1 billion dollars and George Mason University roughly $400 million. A portion of this funding is for construction. Nonetheless, Virginia is making significant investments in, broadly, computing, data, cyber-related initiatives. Maryland and USM need to be competitive with Virginia and its university system. The Attorney General agreed that Maryland is not providing comparable levels of support and is out of step with other states.

Bel Leong-hong, chair of the Economic Development Subcommittee

Ms. Leong-hong noted that the subcommittee continues to discuss a variety of initiatives important to the cyber economy in Maryland. At the top of its list is raising the alarm about the slowness of the federal security clearance process and the need to expedite it. She noted a recent meeting that she and others had participated in with Congressman Ruppersberger.

Susan Rogan, chair, Subcommittee on Public and Community Outreach
Ms. Rogan reported that her subcommittee is compiling resources for the repository that particularly address the needs of individual consumers. She also noted that the subcommittee is discussing ways to do outreach to small- and medium-size businesses to bring practical take-aways directly to them.

Other Business

Dr. von Lehmen outlined a proposal to prepare for the report on the Council's activities, due to the General Assembly no later than July 1, 2019. He suggested that the report not only look backward to the last two years but also look ahead to the next two years and areas of concern that the Council would like to address. Accordingly, he proposed the following work schedule:

- **February – early May, 2019**. Subcommittees meet to prepare for Council's May 22 meeting.
- **May 22, 2019**. Meeting purpose. Each subcommittee proposes new recommendations or broad areas of concern, if any, that it will take up in the 2019 – 2021 period of the Council's activities.
- **June 3 – June 12**. Draft activities report will be circulated to the subcommittees for comment.
- **June 14 – June 25**. OAG Review
- **June 26-27**. Document finalized and copies submitted to the General Assembly NLT Friday, June 28.

There were no objections to the proposal. There being no further business, the meeting was adjourned at 1:50 pm.