Summary
Maryland Cybersecurity Council Meeting
October 25, 2017
10:00am – 12:00pm
University of Maryland University College
Adelphi, Maryland

Council Members Present or Represented (34/57)
Attorney General Brian Frosh, John Abeles, David Anyiwo, Antonin Dahbura, Robert Day, Cyril Draffin, Patrice Drago (for Delegate Carey), David Engel, Judith Emmel, Howard Feldman, Michael Greenberger, Clay House, Teri Jo Hayes, Brian Israel, Jonathan Katz, Miheer Khona, Walter Landon, Michael Leahy, Senator Susan Lee, Belkis Leong-hong, Blair Levin, Larry Letow (by phone), Ken McCreedy, Joseph Morales, Rajan Natarajan, William Pallozi, Jonathan Powell, Jonathan Prutow, Markus Rauschecker, Sue Rogan, Senator Bryan Simonaire, Russell Strickland, Steven Tiller, Carl Whitman.

Staff Attending
Tiffany Harvey (Chief Counsel, Legislative Affairs, OAG), Rich Trumpka (AAG, OAG), Jeff Karberg (AAG, OAG), Charles Ames (Director, Cybersecurity, DoIT), Howard Barr (Principal Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Dr. Greg von Lehmen (Council Staff, UMUC).

Invited Guests
Rick Wilson and John Kerr, Federal Data Systems

Council Meeting

Remarks by the Attorney General
The Attorney General welcomed all in attendance, thanking Council members for their commitment and other attendees for their interest in cybersecurity issues. He noted that the purpose of the meeting was to kick-off the Council's work for the new year and stated that he looked forward to the subcommittee report-outs.

Administrative Matters.
The Attorney General congratulated member Michael Leahy on his full appointment as DoIT Secretary and recognized recently appointed members to the Council: State Senator Bryan Simonaire (Critical Infrastructure Subcommittee), Cyril Draffin (Critical Infrastructure), Terri Jo Hayes (Education and Workforce Development Subcommittee), Miheer Khona (Education and Workforce Development), Mathew Lee (Economic Development)

Markus Rauschecker (Critical Infrastructure), Christine Ross (Economic Development) and Stacy Smith (Economic Development). He also mentioned that Sally Guy would be the Department of Legislative Services' liaison to the Council.

He called for the minutes of the June 1, 2017, meeting and asked if any members had objections to approving them. There being none, the minutes were unanimously approved.

Announcements.
The Council's legislative reception and meeting in Annapolis will be on Thursday, *January 25, 2018 in the Miller Senate Building*: 11:30 am – 1:00 pm (reception) and 1:00 pm – 2:00 pm (meeting).

Updates

1. The Equifax breach. The Attorney General briefly reviewed the engagement his office has had with Equifax and the actions his office has taken to advise consumers of the facts about the breach and steps they can take to protect themselves. This included the production of a video posted on the AG's website that was shown to the members. Mr. Rich Trumpka and Mr. Jeff Karberg from OAG made presentations to the Council to provide additional details. Key takeaways for the Council were the following.

<u>Mr. Trumpka</u>

- 145 million people were affected, including 3 million Maryland citizens.
- The breach was made possible by the failure of Equifax to apply a patch compounded by the fact that the company's vulnerability scans did not identify the lack of a patch as a problem.
- It appears that company announced the breach about six weeks after it had been discovered. The chronology will be important to determining whether the firm met state notice requirements.
- The Attorney General's intervention was instrumental in Equifax including other languages besides English on its consumer website and in ceasing to obscure the free remediation it was offering by steering concerned consumers to products the firm wanted to sell.
- Equifax has indicated that for those affected it will be offering free credit locks for life. OAG will be reviewing that offering, since it is unclear whether a 'lock' is the same thing as a 'freeze'. It's already known that the lock will not have a PIN associated with it.
- Under Maryland law, freezes in cases like this must be free but charges still apply to thaws. Eliminating the cost for thaws might be something for the Council to propose.

<u>Mr. Karberg</u>

- Unlike the Target breach or others, this breach was different in that many people affected had entered into no transaction with Equifax.

- The insecurity hanging over affected people has no end date since the information cannot be put back into the box. This could be more than an inconvenience for consumers—especially those on fixed incomes—who may be paying for freezes and thaws throughout their lives.
- The call centers established by Equifax are inadequate and present a barrier to relief by older citizens who do not have or use computers.

2. The Governor's Executive Order on Cybersecurity. The Attorney General noted that the executive order instructs the Office of Homeland Security to create a cybersecurity plan and stated that the Council will work cooperatively with OHS to create the best possible product for Maryland.

3. The foreign interference with US elections and Maryland election security. The Attorney General observed that this of course is a concern for everyone. While he cannot judge whether the efforts made by the State Board of Elections are the right efforts, he was convinced that it understood the challenges and was making a good faith effort to address them. He indicated that SBE would make a presentation at the January meeting of the Council.

In response to the Attorney General's comments, Mr. Brian Israel remarked that a key strength of Maryland's election process is the use of the paper ballot that should be preserved.

Subcommittee Reports

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

Senator Lee indicated that both she and her co-chair, Mr. Blair Levin, had a number of meetings with the subcommittee that produced a robust roadmap for the upcoming year:

- Cyber First Responder Reserve. *July 2017 Activities Report,* (p. 10). The subcommittee will aim to complete its research on this recommendation and to offer a proposal this session or next that might be useful to the executive branch as it begins to implement the governor's recent executive order on cybersecurity.
- Legislation to create a civil cause of action for unauthorized computer intrusion (p.11). The subcommittee believes that the common law remedies are not effective as indicated by court decisions in other states.
- Legislation to extend the no-charge credit freeze option (p.11) in the 2017 law to minors and to eliminate the charge for corresponding thaws. Senator Lee noted that the importance of the 2017 legislation is underscored by the Equifax breach.
- Legislation to encourage the adoption of the NIST Framework in the State IT Master Plan (p. 12).

- Legislation that would extend breach notification requirements to the judiciary and the legislature (p. 20). This proposal would apply to the other branches a duty that already applies by law to the executive branch and to private sector entities.
- Legislation to require state procurements to incorporate an independent security review and to certify an appropriate level of security prior to government acceptance (p. 20). The subcommittee recognizes that the similar legislation pertaining to procurement by the national government is likely to pass the US Congress.
- Legislation that would require ISPs to have a consumer's express consent to sell their browsing history (p. 20). The subcommittee is mindful that Minnesota already has enacted legislation to this effect, that other states are likely to follow, and that such a requirement is necessary to give consumers control over potentially very sensitive information.
- Legislation that would make extortion through ransomware a crime and levy increasingly heavy penalties, depending on harm caused (p. 20).
- Background research that would inform legislation requiring consumer labeling indicating the security level of IoT devices (p .21). The subcommittee acknowledges that this is a complex issue, requiring technical definitions, qualitative judgements about where to draw the line on security 'levels', and a way of communicating the information in a concise and easily understood manner. The subcommittee does not anticipate advancing a legislative proposal in this regard in the 2018 session.
- Legislation to ensure the transparency of data held by data brokers and the right of consumers to correct incorrect information (p. 21).

DoIT Secretary Michael Leahy, chair, Incident Response Subcommittee

Secretary Leahy called on Charles Ames, DoIT Director of Cybersecurity, to provide an update on DoIT's cybersecurity initiatives. Mr. Ames used a short PowerPoint presentation to make several key points:

- As a recap, he noted that 2016 was a year of planning and some improvements in the state's cybersecurity posture. The planning was informed with a risk assessment framework to identify and prioritize needs and investments.
- To help the Council visualize where the state is, he walked the members through two maturity models, each describing a continuum from very basic to very advanced capabilities. He indicated that most states, including Maryland, are at a nascent level.
- Based on data he collected across 21 states, the average annual state cybersecurity budget is $6.5 million, with a standard deviation of $4 million.
- To move the Maryland to a high level of maturity, his planning effort estimates it would cost $28.9 million in one-time investments with a sustainment budget of about $14 million to $15 million a year afterwards. These would carry the state to better threat monitoring, proactive capabilities and threat intelligence and data analytics.

The Attorney General asked where Maryland ranked in terms of state expenditures on cybersecurity. Mr. Ames answered that the state is at the low end with a cybersecurity budget of

about $3.8 million. He noted that next budget ask would be $10 million, with the normal uncertainty around the outcome. The Attorney General asked Secretary Leahy if he would welcome an endorsement from the Council of the funding levels DoIT believes it needs for cybersecurity. The Secretary indicated that such would be very helpful, adding that in looking at other states, like Arizona and Oklahoma, he thought it might be possible to ramp up quickly for less than their initial estimates.

Senator Simonaire referenced the fact that some state agencies had been holding more personal identifying information (PII) about Maryland citizens than necessary and asked Secretary Leahy what role DoIT has across the executive branch in data governance, monitoring of networks across state agencies, and training of agency staff. The Secretary stated that DoIT's mandate is to standardize data governance across all agencies and to bring agencies into a true enterprise system. To the extent that agencies do not come into that system, he emphasized that they would be held to the same baseline security required of everyone else. With respect to the security of PII in particular, he underscored the seriousness of that responsibility and that DoIT was taking active steps to address it. Finally, he answered that DoIT does offer training and that some agencies have availed themselves of it.

Mr. Levin asked Secretary Leahy, if he thought he could accomplish his goals with less than the figures suggested, then what investment would be necessary over one or two years to raise the level of state capabilities and what would be the sustainment budget in the succeeding years? The Secretary answered that a foundational investment over one or two years would be necessary. He explained that he thought the cost of that investment could be brought down by leveraging the experience of other states and consolidating the licensing of security tools used by different Maryland agencies, for example. He mentioned that timing was important and that it would be better to have the executive branch on one enterprise system so that solutions can be global and economies of scale achieved rather than taking a piecemeal approach.

The Attorney General reiterated that the question of the state's cybersecurity budget could be one on which the Council might be helpful. Understanding that the Secretary would recuse himself, the Attorney General asked whether any of the other Council members had any objection to writing a letter to the Governor recommending increased funding for the DoIT's cybersecurity budget. Hearing none, the Attorney General asked Dr. von Lehmen to draft a letter to that effect and to circulate it to the Council for comment.

Mr. McCreedy commented that he hoped due consideration would be given to the cybersecurity capabilities of Maryland firms to assist the state rather than defaulting to large out-of-state vendors. Mr. Abeles mentioned the Continuous Diagnostics and Mitigation Program (CDM) of the federal government and asked whether the state could participate in that program to access the tools that it makes available. Mr. Ames stated that the price tag for participation is high and as far as he knew the program was offered only to federal agencies. However, he indicated that he would confirm whether that was the case and report back. Mr. House suggested that the

Council's letter to the Governor reference not only the initial investment but also the importance of sustainment funding since security tools are expensive to run.

Professor Michael Greenberger, Critical Infrastructure Subcommittee

Professor Greenberger noted that the subcommittee had executed on Recommendations 8 and 9 in the last year, as captured by the *July 2017 Report*. Specifically, it assembled an initial collection of resources and best practices for infrastructure owners (Recommendation 8) and similarly compiled the latest information about the conduct of risk assessments to be made available to critical infrastructure stakeholders to encourage risk assessment (Recommendation 9). He noted that all these materials would be hosted in a repository on the Council's website. Finally, he noted that the subcommittee had analyzed the interdependency of the various sectors for the efficient conduct of protection and risk assessments and included these findings in the *July 2017 Report*.

Going forward, Professor Greenberger indicated that the subcommittee would focus on three activities within *Report*:

- First, it will continue to add resources to the repository. He suggested that the subcommittee be the entity to review additions proposed by others.
- Second, it will focus on the important need for information sharing. Specifically, it is looking at ISAOs -- information sharing analysis organizations -- and the creation of cyberinformation sharing and collaboration programs which follow the DHS model. He noted a proposed model for information sharing that Mr. House had sketched out.
- Third, he noted that the subcommittee has been discussing the issue of election security and whether it should be an area of investigation for the subcommittee or the Council. Given the sensitivity of the issues, he urged that this not be a subject of debate this meeting, but that the Council continue to look at it, monitor it and possibly raise it as an item for the January meeting or soon thereafter.

Dr. Katz asked if the repository was operational and whether, in addition to very long and complex documents, shorter resources focused on simpler immediate steps to improve cybersecurity will be included. Professor Greenberger stated that he thought the suggestion was an excellent one that the subcommittee would discuss. He deferred to the report-out of the Subcommittee on Public and Community Outreach on the timeline for the repository's operation.

On the election security issue, Mr. Ames asked whether the Council was really equipped to be helpful, given the sensitive information about its networks could not be brought into an open forum. Professor Greenberger suggested that the Council could be helpful at the level of compiling and recommending best practices.

Professor Jonathan Katz, Education and Workforce Development Subcommittee

Professor Katz provided a summary of closed items and open items from the original six recommendations of the subcommittee:

Recommendation 10 (Basic Cybersecurity Education). Professor Katz noted that there were many efforts already underway in the state and nationally that intersected with Maryland. For this reason, the item was closed in the July 2017 report as superseded by other developments.

Recommendation 11. Maryland Scholarship for Service Program. The concept is to duplicate the federal scholarship-for-service program and to fund it either by reprogramming state scholarship dollars and/or by recommending new state funding. Professor Katz stated that to advance this recommendation, a meeting with the MHEC Secretary or his staff will be planned.

Recommendation 13. Study of Cybersecurity Workforce Skills and Needs. As part of its due diligence, the subcommittee became aware of a jobs heatmap created by NIST's National Initiative on Cybersecurity Education (Cyberseek) through a grant to Burning Glass and CompTia. The site provides current and very granular information about cyber workforce needs that are keyed to the Cybersecurity Workforce Framework. This item was also closed in the 2017 Report.

Recommendations 12 (Resources for University Computer Science departments) and Recommendation 15 (Increased Funding for Academic Research). Using University of Maryland, College Park, as an example, Professor Katz noted that enrollments in computer science and cybersecurity have grown dramatically and that resources to sustain these programs has not grown accordingly. Classes at the senior level has as many as 80 to 100 students. To shed light on this issue, as well as greater support for cyber research by the state, the subcommittee is considering studies that would compare Maryland with what other states are doing.

Recommendation 14 (Transition Path for Community College Graduates). There are universities within USM that have articulations in cybersecurity with community colleges. But this does not seem to be the case for the more technical programs in the field. The subcommittee has become aware of a pilot effort to create such a pathway and is in discussion about how to support this effort.

Senator Simonaire noted the efforts of his employer, Northrop Grumman, to support K-12 cybersecurity education. He asked Dr. Katz if he knew of other firms that did this and whether there is any effort to educate younger students about how their behaviors can affect their ability to get a security clearance. The Senator noted that many cyber jobs require such clearances. Professor Katz was sure other firms are involved in supporting K-12 computer science and cybersecurity education but was not aware of a list of such firms. As someone who has held a clearance, he agreed completely with the importance of security clearances in the field. Mr.

Israel shared that a Maryland firm, LifeJourney, is a platform about cybersecurity job roles that serves many schools. It incorporates an exercise that shows students how their digital footprint could affect their chances of getting a security clearance.

Bel Leong-hong, Chair, Subcommittee on Economic Development

Looking at the last year, Ms. Leong-hong noted the success of Delegate Carey's bill in the last session to extend the tax credit to firms for the cost of security clearances. This was a need that the subcommittee and others had identified and had proposed to the Council for action. Looking ahead, she indicated that the subcommittee will focus on the following major initiatives:

- A mechanism for funding a) an executive loan program and b) internships and apprenticeships in cybersecurity that could serve as avenues for security clearances.
- A mechanism for supporting the growth of smaller firms providing cyber products. Discussed was a tax credit to incentivize Maryland firms to purchase cybersecurity products from other Maryland firms developing them.
- A mechanism for creating a funding pool to subsidize cybersecurity investments by small firms and to train local law enforcement in responding to cyber attacks.
- An income tax credit for cybersecurity professionals who relocate to Maryland to fill cyber positions.

Sue Rogan, chair, Subcommittee on Public and Community Outreach

Ms. Rogan reported that the repository mentioned by Professor Greenberger is expected to be operational in November. It will initially include the many resources developed by his subcommittee. It will later add others compiled by her subcommittee or anyone else who identifies resources of value. She noted that equally important to launching the repository is advertising it so critical infrastructure providers, small and medium businesses, and consumers are aware of it. Accordingly, her subcommittee will compile a plan for doing this. She indicated that the subcommittee would be looking at other outreach opportunities to recommend to the Council.

Finally, Ms. Rogan announced that members of her subcommittee helped arrange a webinar on cybersecurity and nonprofits with an expert from Johns Hopkins. This was recorded and will be distributed to the nonprofit community in some way.

<u>Guest Presentation on Cyber Vulnerabilities of First Responders</u>.

The Attorney General introduced Mr. Rick Wilson, senior vice president of technical solutions at Federal Data Systems. Mr. Wilson had careers in the Air Force and NSA and had served as a Laurel city councilman. The Attorney General also acknowledged Mr. John Kerr who accompanied Mr. Wilson.

Mr. Wilson used a 2014 incident in Centerville Louisiana to illustrate that first responder cyber vulnerabilities are not hypothetical. In this case, social media and fake news were orchestrated to create a perceived local emergency and to provide false instructions to the local population. The result was general confusion and hours of effort by local authorities to bring the situation under control. He noted that the attack was traced to an adversary nation state. Given what the nation has seen more recently in disruptive DDoS attacks and major intrusions, the scenarios can be much worse.

Mr. Wilson then discussed some of the first-responder vulnerabilities and the reasons for them. The fundamental problem is that local jurisdictions do not have the staff, the expertise, or budget to keep their networks secure or to defend against an attack. The normal ways in which everyone operates create other vectors for attack. For example, responders keep names and numbers of other responders on their cell phones, which can easily be harvested for misuse in a future emergency. That emergency could be something as normal as a winter snowstorm or it could be something that is orchestrated and is much more threatening.

He suggested several steps that could improve the level of security beyond the cyber workforce development efforts already underway in the state:

- Bring the issue of network and communications vulnerability into discussions with state and local responders.
- Introduce failed networks into exercises that state and local responders do each year so that the vulnerability is recognized and resiliency can be practiced.
- Amend Section 508 (Senator Amoss Fire Apparatus Funds) so that monies from the fund can be used for network security improvements. There are two approaches for getting better security. One is for localities to contract with one or more private vendors. The other, now being tried in some states, is to create a state-level public service network that local jurisdictions could buy into and use in lieu of their own networks.

Mr. Levin asked whether the federal-state effort called FirstNet solved the problem of communications vulnerability. Mr. Wilson answered that it does not. FirstNet is one piece of a system the security of which depends on the security of the larger network.

<u>Other business</u>

Dr. Kornegay from Morgan State was listed on the agenda to announce the new cybersecurity lab at Morgan State University. Since he was unable to attend the Council meeting, Dr. von Lehmen and Mr. Ken McCreedy commented on the lab. Mr. McCreedy noted that the distinctive feature of the lab is its focus on IoT security.

Dr. Dahbura from Johns Hopkins asked to make a final comment about the Equifax breach. He stated that the burden of securing credit records should not fall on the affected consumers and

underscored the problems this creates in a diverse society where many consumers may not understand what they need to do.

The Attorney General observed that his office normally does not announce investigations, but he wanted the Council to know that he and the AGs of other states are investigating Equifax and hope to produce remediation for those affected. Second, he noted that the next session of the legislature is likely to produce a number of bills from Senator Lee and others that further ease credit freezes and thaws and raise the bar of responsibility of firms that collect and broker extremely detailed information about people.

There being no further business, the Council was adjourned at noon.