Summary
Maryland Cybersecurity Council Meeting
January 25, 2018
1:00 pm – 2:00 pm
Senate Miller Building (West II)
11 Bladen Street
Annapolis, Maryland

Council Members Present or Represented (32/57)

John Abeles, Don Fry (for Attorney General Brian Frosh), Cal Bowman (for Pete Landon), Kevin Crain (for Kristin Jones Bryce), Kara Contino (for Senator Bryan Simonaire), Brian Corbett, Cyril Draffin, Patrice Drago (for Delegate Ned Carey), Antonin Dahbura, Anupam Joshi, Judi Emmel, David Engel, Terri Jo Hayes, Clay House, Tami Howie, Brian Israel, Ken McCreedy, Miheer Khona, Dr. Kevin Kornegay, Anthony Lisuzzo, Senator Susan Lee, Blair Levin, Joseph Morales, Rajan Natarajan, Jonathan Powell, Jonathan Prutow, Markus Rauschecker, Sue Rogan, Christine Ross, Lance Shine (for Secretary Leahy), Stacey Smith, and Steven Tiller.

Staff Attending

Tiffany Harvey (Chief Counsel, Legislative Affairs, OAG), Howard Barr (Principal Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Dr. Greg von Lehmen (Council Staff, UMUC).

Guest Speaker

Nikki Banes Charlson, Deputy Administrator, State Board of Elections

Council Meeting

Opening Remarks by the Chair

Mr. Don Fry chaired the meeting for the Attorney General who was unable to attend. In calling the Council to order, he reminded that the agenda was for one hour instead of two in light of the preceding legislative reception and noted a change in the order of items to permit the guest speaker to come before the subcommittee reports. With those preliminaries covered, he called for the minutes of the October 25, 2017 meeting. There being no discussion, motions were made, and the minutes were approved.

Guest Presentation on the Maryland Election Security

Mr. Fry welcomed Ms. Charlson and thanked Ms. Linda Lamone (State Administrator of Elections) who was present for making Ms. Charlson available to speak. Ms. Charlson indicated that while her remarks of necessity would be at a high level, they would still be informative about SBE's efforts to secure the State's election and voter registration systems.

In general, she noted the following about SBE's approach to cybersecurity:

- SBE's security planning is anchored in a risk assessment of their systems. This has informed a defense-in-depth of those systems and the data on them.
- Commercial vendors are central to SBE's security strategy. Reliance on vendors enables SBE to benefit from their expertise, infrastructure, and experience with a variety of other clients. For example, a contractor uses data analytics and artificial intelligence to monitor both external interactions with SBE's websites and traffic across its networks on a 24/7 basis. Vendors are also used proactively to identify system-specific vulnerabilities, such as testing the security of the election night network.
- The US Department of Homeland Security (DHS) is an active and highly valued partner by providing services and funding for election security. DHS recently conducted a two-week risk assessment of SBE's vulnerabilities that included susceptibility to phishing attacks. Similarly, DHS helps with the physical security of voting machines by assessing the risk to machines while in storage. When these activities generate findings, SBE systematically acts to resolve them at the state and local board of election levels.
- SBE regards culture as key to security. As an organization, SBE follows cybersecurity best practices. For example, it:
    - Audits monthly computers used at the local board level to ensure that they are patched and updated regularly.
    - Uses independent and redundant security systems. It takes advantage of DoIT's tools and independently runs its own vulnerability scans and penetration tests.
    - Looks for unusual behaviors in the use of the voter registration and absentee voting websites and monthly audits voter registration data.
    - Requires after each election that each precinct compare voter check-in lists against the number of votes cast and explain any discrepancies.
- The state's election systems benefit from environmental awareness. SBE receives threat information from the US Election Assistance Commission and alerts from the Multi-State Information Sharing and Analysis Center. This enables SBE and its local boards to better secure their systems, whether it's by blocking a particular IP address or taking some other action. The federal government is permitting state election officials and other state officers to obtain security clearances so that sensitive threat information from national security sources can be more quickly and more fully shared.

Addressing the state's election systems more specifically, Ms. Charlson noted that SBE's central voting system network is not connected to the internet. The county networks used to copy ballots onto machines, tabulate precinct votes, and aggregate votes to the county level also do not interact with the internet. Thumb drives used to transfer election results from precincts to the counties' closed networks are encrypted and are transported by bipartisan teams.

Unlike the state's election systems, the online voter registration system—used by voters to register and to request a ballot—is necessarily connected to the internet with all of the associated risks. However, to minimize these risks, the voter registration website is hosted by a private firm in Annapolis that specializes in web hosting and web security. Data coming through the website is encrypted. The statewide voter registration database receiving the data sits on network that is not connected to the internet and is only accessible to SBE and the local boards of election. Transactions between the website and the voter registration database are regularly reviewed by staff for unusual or suspicious activity.

As a best practice, Ms. Charlson emphasized that SBE has recovery plans in the event of a serious cyber disruption. At the voting locations, staff protect back-up voter registration lists that are stored on laptops and in paper copy in case the electronic poll books fail. Likewise, if other equipment fails anywhere during an election, SBE's plans call for new equipment to be installed within two hours. (Repaired equipment is not recycled.) In the event that the electronic record of the state's elections is suspect, paper ballots provide a physical record of the vote that can be hand-counted if necessary.

SBE exercises various scenarios from time to time to keep both state-level and local election staff ready for contingencies. Ms. Charlson noted, for example, that she and several other staff participated in a full day of challenging table-top exercises in Boston that were organized by the Belfer Center's *Defending Democracy Project* at Harvard University.

Ms. Charlson concluded by commenting on the suspicious activity on Maryland's online voter registration website in August 2016. She pointed out that the source IP address was automatically blocked by security software and that subsequent analysis by the FBI and other federal teams indicated that no breach had occurred. As a precaution, the vendor hosting the website conducted an analysis of several months of data preceding the August event and uncovered no evidence of a breach. She reiterated that security training is a constant at both the SBE and local election levels to maintain alertness. Likewise, they closely manage their service agreements with vendors to ensure that they are keeping their software patched and up-to-date.

In response to her presentation, a number of Council members raised questions:

- Professor Joshi (UMBC): Was there any attribution of the specific activity directed against Maryland? Ms. Charlson: SBE did not make any attributions itself, but DHS and other agencies concluded that the source was Russia.
- Professor Dahbura (Johns Hopkins University): Does SBE have staff specifically dedicated to cybersecurity? Ms. Charlson: SBE has four or five full-time IT staff, none of whom is solely dedicated to cybersecurity. However, she reminded that SBE's vendors have teams specifically focused on the security of the systems that they provide.
- Ms. Tamie Howie (Maryland Tech Council): Is there a problem authenticating persons registering to vote? Has there been a breach of the registration system? Ms. Charlson: The State attempts to secure authentication by requiring two kinds of data: the state driver's license number and social security number. If one or the other is not verified, the

user cannot proceed. Other backend checks are used to verify legitimate interactions with the system. There is no evidence that the voter registration database has been breached.

- Mr. Rauschecker (CHHS): Is there a role for the Council in election security? Ms. Charlson: There is a senate bill that would add SBE to the Council. Whether SBE is or is not on the Council, it is certainly willing to share information as appropriate to support the Council.

<u>Subcommittee Reports</u>

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

Senator Lee indicated that had introduced several bills that aligned with her recommendations of her subcommittee included in the July 2017 Activities Report:

- SB 202 (Consumer Protection - Credit Report Security Freezes - Notice and Fees). This bill would extend the law passed last year (SB 525/HB 974) that provided for no charge for the first credit freeze. Specifically, for affected consumers, SB 202 would prohibit charges for any service related to a security freeze, including placement, temporary lift or removal and would allow parents and guardians similar rights with respect to their minors.
- SB 376/HB 476 (Criminal Law - Crimes Involving Computers - Cyber Intrusion and Ransomware). This bill is a modified version of last year's SB 287/HB 772 and is intended to accommodate concerns of the committees. Addressing cyber intrusion in general, the bill would identify ransomware as a crime and provide a right of private action for unauthorized computer and network intrusion.
- SB 882 (Procurement – Telecommunication and Computer Network Access – Security). This bill has two purposes. In part, it would require the state's procurement of Internet of Things (IoT) devices to meet certain security requirements. In this respect, the bill is modelled on federal procurement regulations and aims to reduce the vulnerability of the state networks to breaches and disruption. In addition, the bill would restore net neutrality in light of the withdrawal of the FCC regulation that would have accomplished the same. The bill is similar to a bill introduced in New York's legislative assembly.

Mr. Fry indicated that members will get advance notice of the hearings, so that any who are interested can give testimony.

Lance Shine, Deputy DoIT Secretary, for Secretary Michael Leahy, Chair, Incident Response Subcommittee

Mr. Schine indicated that there are no updates for the subcommittee.

Mr. Markus Rauschecker for Professor Michael Greenberger, Chair, Critical Infrastructure Subcommittee

Mr. Rauschecker conveyed Professor Greenberger regrets for not being able to join the Council's meeting. He updated the Council on the repository for small- and medium-size businesses that is now live on the Council's website (http://www.umuc.edu/mdcybersecuritycouncil). He noted that with the assistance of CHHS, the subcommittee had contributed a large number of resources for the initial launch of the repository and that it would be submitting additional resources this year. Currently, the site is in a quiet launch phase pending the creation of a critical mass of resources. Mr. Rauschecker suggested that with the next installation of resources the site should be ready for wider dissemination.

Dr. Greg Von Lehmen, Council staff, for Professor Jonathan Katz, Chair, Education and Workforce Development Subcommittee

Dr. von Lehmen reminded that one of the recommendations of the subcommittee in the *July 2017 Activities Report* concerned the creation of a state-level cybersecurity scholarship for service program like the program managed by the National Science Foundation. He stated that to advance this recommendation, a meeting was held in November with Secretary Fielder at the Maryland Higher Education Commission. The Commission manages a number of scholarship programs for the State. With subcommittee support, he noted that Senator Simonaire, and Senator Lee introduced SB 204 (Higher Education - Cybersecurity Public Service Scholarship Program) in the current session. He indicated that he will sending weekly updates to the Council about this bill and others consistent with the Council's recommendations.

Mr. Miheer Khona, for Ms. Bel Leong-hong, Chair, Subcommittee on Economic Development

Mr. Khona noted that Ms. Bel Leong-hong had experienced a loss in her family and was unable to join the Council's meeting. His update for the subcommittee was the following:

- To incentivize investment in cyber start-ups, the subcommittee had recommended that the current investment tax credit should be available to the investors in a firm rather than to the Maryland firm itself. Mr. Khona explained that as the tax credit now stands, start-ups are not able to take advantage of the tax credit since they do not show a profit. He noted that Senator Guzzone has proposed SB 228 (Cybersecurity Investment Incentive Tax Credit – Eligibility, Appropriation, and Sunset Extension) to switch the credit to investors. Last year, the bill failed, but there was some optimism that it would succeed this year.
- The subcommittee has also recommended a tax credit to Maryland businesses purchasing services and products from Maryland cyber firms. To achieve this purpose, HB 364/SB 310 (CyberMaryland Act of 2018) has been introduced this session on behalf of the administration.

Mr. Khona concluding by observing that the subcommittee supports the Excel Maryland finding that Maryland would benefit from a ‘hub’ or one-stop shop for investors to provide comprehensive information about the state’s business incentives, which companies are in start-up mode, introduce investors to companies or entrepreneurs, and serve as a platform for other services. However, it did not expect legislation to be introduced this session that would establish such an entity.

Mr. Fry emphasized the importance of HB 364/SB 310 including the purchase of cybersecurity services as well as products for purposes of a tax credit. This is because small- and medium size firms often contract for IT and cybersecurity services instead of standing them up in house.

Sue Rogan, chair, Subcommittee on Public and Community Outreach

Ms. Rogan updated the Council on the next steps in connection with the repository. In addition to building out its resources, she indicated that the criteria for resource selection would be tightened to focus especially on small- and medium-size business and that there would be user testing to see what changes might make the search interface easier for businesses to use. She thanked CHHS for its bibliographic work and UMUC for designing and launching the site.

Mr. Fry expressed his appreciation for Ms. Rogan’s leadership and the subcommittee members for their work.

<u>Other Business and Adjournment</u>

Mr. Fry thanked the members for their presence at the reception and the meeting. He congratulated the Council on the fact that the reception attracted a significant number of legislators and staffers. He also observed how important it was that the speaker, Ms. Deborah Plunkett, provided a third-party validation of a number of the Council’s concerns and recommendations.

Hearing no other business, he adjourned the Council at 1:40 pm.