Draft Meeting Minutes
Maryland Cybersecurity Council
9 June 2021 Meeting
Zoom Format

The following is an outline of the meeting.
The full meeting recording and speaker slides may be found here.

Council Members Present or Represented (43/57)
Attorney General Brian Frosh (Chair), John Abeles, Dr. David Anyiwo, Barry Boseman, Delegate Ned Carey, Dr. Michel Cukier, Dr. Anton Dahbura, Robert Day, Vince Difrancisci, Cyril Draffin, Patrick Feehan, Howard Feldman, Michael Greenberger, Terri Jo Hayes, Senator Katie Fry Hester, Fred Hoover, Clay House, Mark Hubbard (for Walter Landon), Brian Israel, Anupam Joshi, Miheer Khona, Kevin Kornegay, Linda Lamone, Secretary Michael Leahy, Mathew Lee, Senator Susan Lee, Blair Levin, Bel Leong-hong, Larry Letow, Delegate MaryAnn Lisanti, Anthony Lisuzzo, Rodney Petersen, Jonathan Prutow, Markus Rauschecker, Martin Rosendale, Christine Ross, Senator Bryan Simonaire, Gregg Smith, Russell Strickland, Steven Tiller, Troy Stovall, Paul Tiao, and Pegeen Townsend.

Staff Attending
Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), Laura Corcoran (NSA Fellow, Office of the Attorney General), Thomas Elder (Policy Analyst, Maryland Library and information Services), Hannibal Kemerer (Director, Legislative Affairs, OAG), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Chip Stewart (State CISO), Nithin Venkatraman (Chief of Staff, Office of Senator Katie Fry Hester), and Dr. Greg von Lehmen (University of Maryland Global Campus, Staff to the Council).

Council Meeting

Opening Remarks by the Chair

The Attorney General welcomed the Council and members of the public. He recognized three special guests whom Senator Hester had invited: Delegate Samuel Rosenberg (District 41, Baltimore City), Cole Beauchat representing Delegate Patrick Young (District 44B Baltimore County), and Ben Yelin, Program Director for Public Policy and External Affairs, at the Center for Health and Homeland Security at the University of Maryland School of Law. The Attorney General then announced the agenda, including the speaker, the subcommittee reports, two special reports, and an update on the Council's Activities report due July 1 to the General Assembly.

Subject Matter Expert Presentation

The Attorney General called on Secretary Leahy to introduce the speaker, Douglas Robinson, Executive Director of the National Association of State CIOs (NASCIO), since the Secretary had extended the invitation to speak on behalf of the Council.

Mr. Robinson's presentation ("States at Risk: Cybersecurity Priorities, Trends and Perspectives") was based on the 2020 survey that NASCIO conducted of state CIOs. This was the latest of the biennial surveys that NASCIO has been doing for years. In his presentation, Mr. Robinson discussed the threat landscape, the top priorities of state CIOs as revealed by the survey, the changes in operations introduced by COVID, the CIO business models used across the states, the cybersecurity maturity of state cybersecurity programs, how COVID challenged continuity and amplified gaps in state cybersecurity, and cybersecurity spending trends at the state level.

Council Business Meeting

Approval of minutes. The Attorney General announced a quorum. He called for the minutes of the 25 January 2021 meeting, asking for any discussion. The minutes were approved without objection on motions made and seconded.

Subcommittee Chair Reports

Subcommittee on Law, Policy, and Legislation. Senator Lee reported out on behalf of her co-chair, Blair Levin, and herself. She debriefed on the 2021 session, noting the precautions that had been out in place to protect legislators. A high priority of the session was critical services and police reform. There were two successes in realizing the objectives of two Council recommendations in law this session:

SB 623/HB 425 (Criminal Law - Crimes Involving Computers). Introduced by Senator Lee and Delegate Barron, the law makes possession of ransomware a criminal offense under certain circumstances and provides for increased penalties for possession and use.

SB 49/HB 38 (State Government - Department of Information Technology – Cybersecurity). The law was proposed by Senator Lee and Delegate Carey. It expands the authority of DoIT to advise the General Assembly and the Judiciary on cybersecurity, and in consultation with the Attorney General. to advise and oversee a consistent cybersecurity policy across State agencies and to develop guidance on cybersecurity for local jurisdictions.

Senator Lee noted that other bills related to Council recommendations that she had proposed were not passed:

- SB 112/HB 148 (Commercial Law - Personal Information Protection Act – Revisions). The bill aimed to update the categories of data for which a breach must be reported.
- SB 930 (Maryland Online Consumer Protection Act). The bill would have provided more transparency about consumer data collection by firms and given consumers greater control over their data.

Senator Lee also reported out to the Council four recommendations of the subcommittee for inclusion in the 2021 activities report. She asked Dr. von Lehmen to state those for the record as they were approved by the subcommittee:

- That the State consider incentives for businesses to assess their cybersecurity posture and to invest more, if necessary, to create a cybersecurity program consistent with recognized standards and frameworks.
- That the State consider appropriate legislation to ensure the transparency to consumers of the information held by entities about them and how it is used, the right of consumers to inspect, correct and delete such data, and their right to opt out of the sale of data to third parties.
- That the State consider legislation to enhance the security of Internet of Things (IoT) devices.
- That there be transparency with the State by critical infrastructure providers about compromises that interfere with operations.

Subcommittee on Incident Response. Secretary Leahy noted that the membership of his subcommittee had been changing and that he would be scheduling a meeting in the next few weeks. This would be to discuss governance issues and the enterprise-level approach to cybersecurity and standardization that is the State's best foot forward in terms of cybersecurity. He asked Chip Stewart, the State CISO, to provide other updates:

Machine learning is becoming part of the State's toolset, along with security orchestration and automated response to attacks.

- DoIT is pursuing the "top ten" priorities identified by Mr. Robinson in his presentation.
- The Department has developed a threat intelligence capability by surveilling the dark web for clues about what threat actors may be planning.

Secretary Leahy added that DoIT has moved its Security Operations Center (SOC) into the Department, ending a relationship with a vendor. The in-house SOC offers 24/7 staffing. The change offers DoIT more control and flexibility in responding to needs, since contract modifications are not needed. He also noted that when the subcommittee meets again, he will ask Mr. Stewart to brief them on the SOC.

Subcommittee on Critical Infrastructure. In his updates for the subcommittee, Mr. Rauschecker:

- Recognized the work that Laura Corcoran, the NSA Fellow, had done to date. He noted that she was taking a holistic or comprehensive view of the utility sector serving Maryland. In doing so, she was interviewing people in relevant State agencies, reviewing what other states have been doing, and talking with people in industry. The subcommittee looks forward to her report at the end of the year.
- Highlighted the progress on information sharing recommendation. He observed that threat sharing greatly enhances the cybersecurity posture of organizations. As a result of discussions between members of the subcommittee and the Arizona Cyber Threat Alliance (ACTRA), a white paper was developed that in essence lays out a plan for how to establish an organization like ACTRA in Maryland. The white paper will be included in the Council's 2021 activities report and posted on the Council's website for anyone who would be interested in it.

- The subcommittee is continuing to identify resources that have been added to the repository hosted on the Council's website.

Subcommittee on Economic Development. Ms. Bel Leong-hong noted that during the COVID year many companies were reconfiguring their operations and spending time on related workforce development and improvement. In cybersecurity, the talent gap continues to grow, constituting a persistent brake on growth of the cyber sector in Maryland. For this reason, her subcommittee completely supports the efforts of Senator Hester and the Education and Workforce Development Subcommittee to help address this challenge through efforts like last session's SB 902 (Economic Development - Cyber Workforce Program and Fund – Established).

Regarding her June 2 subcommittee meeting, Ms. Leong-hong mentioned that discussions focused on three topics:

- How to upskill or reskill Maryland residents not currently in IT or cyber jobs to prepare them for those jobs and whether it makes sense to consider ways to attract talent from other states to reside and work in Maryland
- Whether the cap on the size of firms qualifying for the 'buy-Maryland' tax credit should be increased
- To engage with the county-level economic development entities to see how American Relief Act funds can be programmed for cyber workforce development in the State.

Ms. Leong-hong noted that the subcommittee will continue to look at these issues and will invite representatives of several of the county economic development entities to join its summer meeting.

Subcommittee on Education and Workforce Development. Senator Hester summarized the ongoing efforts of the subcommittee to help move the needle on cyber workforce development in the State:

- Building on SB 1049 that did not pass in 2020, the subcommittee undertook expanded due diligence that resulted in SB 902 in 2021. This included discussions with the State of Kentucky about its implementation of the Talent Pipeline Management program developed by the US Chamber of Commerce and a workforce development survey by the Cybersecurity Association of Maryland. The bill aimed to create a partnership including the State Department of Labor, the State Department of Commerce, and private industry to position the State to take advantage of new federal workforce development funds to expand training opportunities in cybersecurity, including apprenticeships, for the unemployed and underemployed. SB 902 came close to passing in the last session and some version of the bill will be proposed again in 2022.

- The subcommittee will meet in July to plan a larger, onsite meeting in the fall. A key purpose of the fall meeting will be in part to bring representatives of State training programs together with industry to raise awareness of those programs.

Subcommittee on Public and Community Outreach. Reporting for Ms. Rogan, the chair, Dr. Anton Dahbura noted various activities in which the subcommittee has been involved:

- It facilitated a cybersecurity webinar on June 2, hosted by Maryland CASH, that focused on cyber crime and featured the Attorney General and Mr. Joseph Carrigan, at the Johns Hopkins Information Security Institute. This was the third webinar the subcommittee facilitate during COVID.
- With the assistance of Dr. Doswell, and as a pilot, the subcommittee has invited students at Bowie State University to serve as externs identifying appropriate resources for the Council's repository. The subcommittee plans to extend the same invitation to students at other HBCUs within the State.
- The subcommittee is discussing how to conduct a survey of individuals and small businesses to gauge their level of cybersecurity awareness. The questions of survey construction, platform, and channels are all part of the discussion.

Special Reports

The State Cybersecurity Study. Senator Hester was given the floor to describe the study. Its purpose is to inform and support a package of bills in the 2022 session to enhance the cybersecurity posture of State and local governments. SB 49 was a 2021 contribution to this objective, but a number of other bills introduced in 2021 that would have carried the work further did not pass.

The study will be co-led by Senator and Ben Yelin at the Center for Health and Homeland Security at the Carey School of Law at the University of Maryland, Baltimore. Partners to the study include Senator Lee, the Maryland Cybersecurity Council, the Joint Committee on Cybersecurity, Information Technology, and Biotechnology; the State Department of Information Technology, the Maryland Emergency Management Agency, and the Maryland Association of Counties. A kick-off meeting would occur shortly. The timeline is for the report to be completed by the fall.

The Critical Infrastructure Study Focused on Utilities. Ms. Corcoran, the NSA Fellow, thanked the Attorney General for the opportunity to provide an update to the Council. She observed that there was no shortage of reminders about he effects of critical infrastructure disruption (attack on the Oldsmar water plant in Florida, the power outages in Texas triggered by the weather, and the Colonial Pipeline shutdown). With respect to her research, she noted that she was currently focused on how Maryland and other states report incidents to regulators, what the barriers to investment in cybersecurity by utilities are, and how critical infrastructure is defined to authorize state action to assist in an emergency. She expressed her gratitude to those on the Council who were assisting her and asked that others who would like to be involved with her study to contact her.

Other Business
The Attorney General asked for an update on the Council's biennial report. Dr. von Lehmen observed that the draft had been released to the full Council for comment and suggested changes

on June 7 and asked that members complete their review by June 16 so that the draft could be updated and given to the Office of the Attorney General for review.

The Attorney General reminded that the next plenary Council meeting is scheduled for October 13 (10:00 am – noon). He noted that the meeting is still planned to be virtual and that the members will be updated on any change to an onsite meeting.

Adjournment
The Attorney General asked if there was other business. Hearing none, the meeting was duly adjourned at 12:04 pm.