Meeting Minutes
Maryland Cybersecurity Council
13 October 2021 Meeting
Zoom Format
The following is an outline of the meeting.
The full meeting recording may be found here.

Council Members Present or Represented (37/57)
Attorney General Brian Frosh (Chair), John Abeles, Dr. David Anyiwo, Dr. Anton Dahbura, Delegate Ned Carey, Dr. Michel Cukier, Jessica Curtis and Bryant Wu (for David Engel), Cyril Draffin, LTC Colin Ferguson (for Adjutant General Timothy Gowen), Donald Fry, Michael Greenberger, Terri Jo Hayes, Senator Katie Fry Hester, Clay House, Mark Hubbard (for Walter Landon), Brian Israel, Anupam Joshi, Dr. Kevin Kornegay, Linda Lamone, Mathew Lee, Senator Susan Lee, Bel Leong-hong, Larry Letow, Blair Levin, Delegate MaryAnn Lisanti, Anthony Lisuzzo, Kimberly Mentzell (for Secretary Kelly Schulz), Joseph Morales, Steven Pennington (for Marty Rosendale), Rodney Petersen, Jonathan Powell, Jonathan Prutow, Markus Rauschecker, Chip Stewart (for Secretary Michael Leahy), Steven Tiller, Paul Tiao, and Pegeen Townsend.

Staff Attending
Howard Barr (Assistant Attorney General and Principal Counsel, Department of Information Technology), Laura Corcoran (NSA Fellow, Office of the Attorney General), Patrice Drago (Chief of Staff, Office of Delegate Ned Carey), Hannibal Kemerer (Director, Legislative Affairs, Office of the Attorney General), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Stacey Volodin (Office of Senator Susan Lee), and Dr. Greg von Lehmen (University of Maryland Global Campus, Staff to the Council).

Council Meeting

Opening Remarks by the Chair

The Attorney General opened the meeting welcoming members and members of the public. He reviewed the agenda and turning to the first item on it, he introduced the speaker, Marcus Sachs, Deputy Director of Research, at the McCrary Institute for Cyber and Critical Infrastructure Security, and Mr. Sachs' topic, cybersecurity in the electric utility industry.

Presentation

Mr. Sachs's extended presentation provided an overview of the electric utility industry and its cybersecurity posture. The following are highlights of his remarks:

- There is a high degree of cooperation across the different power generation regions on cybersecurity. This is because they do not compete for customers, and the interconnections between regions require precise synchronization of systems involved in

power generation and distribution. Inherently, there is a strong safety culture within the industry which has come to include cybersecurity.

- While cybersecurity is a critical concern, utilities must deal with other threats to power distribution. These include animals, lightning strikes, and metal fatigue. Individuals have been involved in copper theft and physical attacks on the utility infrastructure, such as shooting at transformers. Physical security is critical to safeguard against activists or others intending harm from accessing facilities under false pretenses (delivery person or contractor).
- All the utilities participate in the Electric Information Sharing and Analysis Center (E-ISAC). The E-ISAC learned a lot about the Russian attack on the Ukrainian power grid. The attack was facilitated by the use of pirated Windows software that was not patched. The use of pirated software is common in many countries and creates exposure of their critical infrastructure to attack. This practice does not exist in the US power industry.
- The difficulty in recruiting and retaining cybersecurity talent in the utility industry is the same across industries in general. The talent gap is ubiquitous. There is a project underway to introduce cybersecurity into engineering curricula across the nation so that the next generation of operators will be cyber savvy. (In response to questions from Senator Lee and Rodney Petersen)
- As connected technology has evolved, cybersecurity has become more complicated. The industry has an edge challenge in which any Wi-Fi connected device—e.g., a smart meter or a smart home—can become a path to an attack. (In response to a question from Clay House).

Business Meeting

The Attorney General confirmed that a quorum of the members was present. He called for the minutes of the 9 June 2021 meeting of the Council. The minutes were approved without objection.

Report by Laura Corcoran, NSA Fellow to the Office of the Maryland Attorney General

The Attorney General welcomed Ms. Corcoran to the meeting and reminded the Council that she had been working on her report on the electric utility sector serving Maryland since December of last year. He mentioned that she will be returning to the NSA in mid-December. Her overview of her report provided background on the electric utility sector, described challenges in securing the grid and highlight a few of the recommendations her report will make to enhance the cybersecurity of the sector serving the State. Her recommendations touched on regulatory goals, building cyber resiliency, adopting security by design for State-funded, grid-related projects, changes in utility reporting to the Public Service Commission, supply chain policies, and data privacy.

Subcommittee Reports

Five subcommittees had reports for the Council:

*Subcommittee on Law Policy, and Legisla*tion. Speaking for herself and her co-chair, Blair Levin, Senator Lee observed that this month two bills responsive to two Council recommendations had become law. These were the ransomware bill proposed by her and Delegate Barron (SB 623/HB 425 [Criminal Law - Crimes Involving Computers]), and the State cybersecurity bill by her and Delegate Carey (SB 49/HB 38 [State Government - Department of Information Technology – Cybersecurity]. She also mentioned that she spoke at a meeting of the National Conference of State Legislators about the Maryland Online Consumer Protection Act, which had been proposed the last two sessions and would be proposed again in 2022. She noted that among other things, the bill would protect the privacy of minors.

Subcommittee on Critical Infrastructure. Markus Rauschecker provided an update on the additions to the repository of cyber-related resources hosted on the Council's website and curated by externs at the Center for Health and Homeland Security at the University of Maryland Law School. He also mentioned that the subcommittee continues to get updates about the cybersecurity standards work of the Emergency Numbers System Board committee on cybersecurity and to provide input into that work. He concluded by thanking Ms. Corcoran for her forthcoming report and expressed the appreciation of the subcommittee for the insights and the actionable character of its recommendations.

Subcommittee on Education and Workforce Development. Senator Katie Fry Hester noted that the subcommittee had met since the June Council meeting. It received a briefing by Tasha Cornish on the cybersecurity survey that the Cybersecurity Association of Maryland had done of its more than six-hundred member firms. The results underscored the challenges that firms have in finding the cybersecurity talent that they need. The workforce shortage, salaries, and need for security clearances topped the list of challenges. The Senator also mentioned that the subcommittee is looking for ways assisting industry by staging a 'match-making event' between industry and cyber job seekers at CyberMaryland or some other venue. Finally, she observed that the subcommittee continues to support the 2021 SB 902 (Economic Development - Cyber Workforce Program and Fund – Established), which will be reproposed in 2022 in some form.

Subcommittee on Economic Development. Ms. Bel Leong-hong mentioned that the subcommittee had recently met and that there were a number of action items that it would follow up on before the next plenary meeting. She stated that one of these items is to engage with the county economic development organizations since they are at the forefront of the economic development of the State. She also underscored that cyber workforce development is critical to the issue of economic development and that her subcommittee is supportive of the work of the Subcommittee on Education and Workforce Development.

Subcommittee on Public and Community Outreach. Ms. Sue Rogan updated the Council on the survey of the general population it is developing to gauge knowledge of cybersecurity hygiene. The purpose of the survey is to establish a baseline to inform future awareness raising initiatives.

She noted that Dr. Dahbura was leading this effort and that Joseph Carrigan, Senior Security Engineer, Johns Hopkins University Information Security Institute. Ms. Rogan also mentioned that the subcommittee was planning another virtual cybersecurity webinar to co-host with the Attorney General's Office.

Special Update on the State Cyber Study

Senator Hester stated that the ad hoc committee steering group was meeting every two weeks and that study would be completed by mid-December. She thanked Ben Yelin for co-chairing the effort and for the assistance of the Center for Health and Homeland Security at the University of Maryland School of Law for its extern support. She recapped the three components of the study led by Dr. Greg von Lehmen (governance), Mr. Chip Stewart (State Executive Branch Cybersecurity), and Ben Yelin (local government cybersecurity), respectively. She noted that the discussion of local government cybersecurity had been informed by a grassroots effort including surveys of, and meetings with, local CIOs and other staff responsible for cybersecurity. The Maryland Association of Counties, the Maryland Municipal League, the Maryland Association of County Health Officials, and the county emergency management directors were all involved in this process. The Senator mentioned that the preliminary findings and recommendations would be presented at the November meeting of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology. She stated that the President of the Senate and the Speaker of the House had sent a letter to herself and her co-chair, Delegate Young, asking the committee to focus its 2022 legislative proposals on three things in cybersecurity that align with the ad hoc committee's State Cyber Study.

Other Business and Adjournment

The Attorney General announced the plenary meeting dates for 2022, noting that the calendar invitations and the public notice would occur soon. There being no other business, the meeting was duly adjourned at 11:40 am.

[Note: These minutes were approved by the Maryland Cybersecurity Council at its 24 January 2022 meeting.]