Draft Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Critical Infrastructure
Friday, May 5, 2023
1:00 pm – 2:00 pm
Virtual Public Meeting

Member Attendance (6/10)
Markus Rauschecker (chair), Dr. David Anyiwo, Jessica Curtis and Adriana Shockley (for David Engel), Cyril Draffin, and Terri Jo Hayes.

Staff
Howard Barr (Assistant Attorney General and Principal Counsel, DoIT) and Dr. Greg von Lehmen (University of Maryland Global Campus, Staff to the Maryland Cybersecurity Council).

Invited Presenters
Michael Block (Chair, Cybersecurity Standards Committee, Emergency Numbers Systems Board [ENSB]) and Josh Jack (Mission Critical Partners).

Meeting Minutes

1. Mr. Rauschecker welcomed the members and the invited presenters and reviewed the agenda. He noted that the recording of the October 20, 2022, meeting of the subcommittee has been available on the Council website. He reminded that a recording addresses the requirements of the Open Meetings Act Manual.
2. He briefly summarized SB 800/HB 969 (Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023)) that had been proposed by Senator Hester and Delegate Qi and signed into law by Governor Moore. He underscored the various recommendations from the Council's grid report that the bill incorporated. He then asked Mr. Draffin and other members of the subcommittee's working group that had advised Senator Hester on the bill to add any comments that they wished to make. Mr. Draffin remarked that the bill was a team effort and that what is important now is the implementation. Ms. Hayes said that the process of informing the bill was systematic, and she commended the leadership of Senator Hester throughout that process.
3. Mr. Rauschecker asked Mr. Block and Mr. Jack to provide an update on the work of the ENSB Cybersecurity Standards Committee. He noted that SB 339 (Public Safety – 911 Emergency Telephone System), passed in 2019, directed the ENSB to consult with the Maryland Cybersecurity Council on cybersecurity standards for the State's NextGen 911 system. The periodic updates for and discussions with the subcommittee were a means of meeting this requirement.

Mr. Block and Mr. Jack observed that the ENSB was engaged in a statewide effort to conduct a cybersecurity assessment of all 24 public safety answering points (PSAPS). The assessment is based on the Cybersecurity Framework (CsF) created by the National Institute of Standards and Technology (NIST) for critical infrastructure. This assessment will guide enhancements to PSAP cybersecurity practices. They noted that each PSAP has a cyber incident response plan in place. Regarding the transition from the legacy systems to NextGen 911, Mr. Jack stated that seventeen of the twenty-four PSAPs were currently on the new system and that all twenty-four would be converted by the end of the calendar year.

4. Mr. Rauschecker thanked Mr. Block and Mr. Jack for their information and commended the use of the CsF as an appropriate national framework for the assessment of PSAPs. He looked forward to a high-level follow-up report on the changes made or planned as a result of the assessment. He turned to the next agenda item—the next critical infrastructure research project to be sponsored by the subcommittee with support by the Attorney General's Office.

   He suggested that the project focus on the cybersecurity of the water utilities serving Maryland. Attacks on these utilities—including one in Maryland—had been reported. The Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert regarding this sector. He expressed agreement with Ms. Hayes' earlier comment that the process that resulted in the grid report was a good model for the Council and benefited the State. He proposed that the same process be followed in this case. Specifically, he noted that the Office of the Attorney General is willing to submit a request for another NSA Fellow to study the water utilities serving the State and to make recommendations to enhance their cybersecurity.

   Mr. Draffin stated that the proposal has merit. Such a report and its recommendations could be of great value to the Public Service Commission in its regulation of these entities. He noted that there is a mix of large and small utilities serving Maryland with a range of cybersecurity practices among them. It would be useful to pin down what the needs are, including the qualifications of staff responsible for the cybersecurity of these utilities. He observed that the EPA has some oversight in this area—he referred to the EPA's latest guidance—but pointed out that the guidance leaves it to the states to determine what the cybersecurity standards and practices should be.

   Ms. Hayes also agreed with the proposed focus. Such a study could identify the biggest threats, the most concerning exposures, and the security improvements that would yield the biggest impacts. She noted that the PSC will have a lot of work to do with respect to cybersecurity and that a report with recommendations could be helpful to it.

   Dr. Anyiwo likewise supported the proposal. He underscore that nation state adversaries were targeting the water utilities sector and that it is crucial that they have appropriate countermeasures in place.

Mr. Rauschecker thanked the subcommittee members for their comments. He asked if there were any objections to the proposed project focus. Hearing none, he asked the members to share any additional thoughts they might have to flesh out the scope of work for the study. He asked Dr. von Lehmen to incorporate these into a draft for the Attorney General's Office. He also requested that Dr. von Lehmen send out a copy of the recent EPA cybersecurity guidance to the subcommittee members.

He asked if there was other business that the members might have. There being none, the meeting was adjourned at 2:10 pm on motions by Mr. Draffin and Dr. Anyiwo.