Meeting Minutes
June 15, 2023
Maryland Cybersecurity Council
College Park Marriott

Council Members Present or Represented (29/56)
Hannibal Kemerer (for Attorney General Anthony Brown, chair), John Abeles, John Bruns (for Secretary Savage), Tasha Cornish, Jessica Curtis (for David Engel), Marcia Deppen (for Secretary Russ Strickland), Dr. Anton Dahbura, Cyril Draffin, Howard Feldman, Lt. Col. Colin Ferguson (for Adjutant General Janeen Birckhead), Adam Flasch, Captain Ronald Fisher (for Major Tawn Gregory), James Foster, Terri Jo Hayes, Senator Katie Fry Hester, Clay House,

achieve this goal that will threaten contemporary cryptography and therefore the security of data and systems in government and industry.

NIST began considering this problem in 2016 and in 2017 launched an effort to develop quantum proof encryption. The process has been “open, transparent, and traceable” so that the foundations of the solutions are fully revealed and testable.

are. Most nations have committed to adopting the NIST standard because of its transparency. In regard to the second question, Mr. Scholl observed that it is true that the four solutions NIST had proposed in the next to final round included one that was actually breakable. However, NIST had asked everyone participating in the process to test those four and that’s where the one defective candidate was discovered. On the one hand, it was concerning that the weakness of that one solution was not discovered until very late in the process, but on the other, the discovery provide that the crowdsourcing process ultimately worked.

There being no further questions, Mr. Kemerer thanked Mr. Scholl for his presentation.

Council Business Meeting

Mr. Kemerer confirmed with Dr. von Lehmen that a quorum of the members was present and called for the minutes of the October 20, 2022, meeting. There was no discussion, and the minutes were unanimously approved on motions from Ms. Leong-hong and Dr. Joshi.

Mr. Kemerer provided the Council with two updates.
• Membership. He noted that a number of new members will be joining the Council. It had lost a several elected representatives for various reasons—Senator Lee and Delegates Carey and Lisanti. A number of other seats have become vacant due to other reasons, like changes in employment and retirements. The Attorney General will follow the statutory procedures for filling the needed seats.

• NSA Fellow Application. In consultation with the Critical Infrastructure Subcommittee, OAG has decided to apply for another NSA Fellow to work for a year on an infrastructure security project. The Council saw the benefits of this program very clearly with Laura Corcoran, and the NSA also saw Laura’s experience as beneficial to her career development and to the Agency. While not certain, the initial indications are that the NSA will be able to provide another Fellow.

<u>Subcommittee Reports</u>

Subcommittee on Law, Policy, and Legislation. Mr. Feldman the

[illegible] Mr. Feldman

Subcommittee on Incident Response. Updates were provided by Ms. Deppen and Mr. Bruns. Ms. Deppen stated that the Cyber Preparedness Unit (CPU) within MDEM was in the process of building out its staff from two to six staff members. The CPU is working with county and municipal governments and state agencies. She noted that it had recently delivered a cyber security exercise to BWI and the MAA. In addition to this work, MDEM is supporting two federal grants for state and local government cybersecurity. Eighty percent of the funds flow to local units of government for investment in cybersecurity. The state has received $3.8 million to date and expects roughly twice that amount in FY 24. She mentioned that MDEM is also administering the $3.6 million Local Cybersecurity Fund that was created in 2022 as one element in the comprehensive cybersecurity legislative package that was passed that year.

Mr. Bruns noted that Secretary Savage had signed off on minimum cybersecurity standards that are mandatory for all Executive Branch departments and agencies. These standards are informed by the NIST Cybersecurity Framework (CsF). In addition, he stated that his office has 20 new PINS that will add to his current security team of 50-60 members. He had recently hired a new director of cyber resiliency who leads DoIT's Security Operation and Incident Response Center who will also support departments in conducting business impact analysis and developing business continuity plans.

Subcommittee on Critical Infrastructure. Reporting for the subcommittee, Mr. Draffin highlighted the significance of SB 800/HB 969 (Public Service Commission – Cybersecurity Staffing and Assessments (Critical Infrastructure Cybersecurity Act of 2023). The bill was proposed by Senator Hester and enacted in the 2023 session. It incorporates key recommendations of a report compiled over a year by the previous NSA fellow, Laura Corcoran. Mr. Draffin mentioned that a working group of the subcommittee had also informed aspects of the bill and will continue to monitor its implementation by the PSC.

In other updates, he mentioned that the subcommittee has continued to track the progress of the ENSB's effort to implement cybersecurity standards as part of its rollout of the NextGen 911. He noted that state law requires the ENSB to consult the Council on its standards. With respect to the new NSA fellow application that Mr. Kemerer had noted, Mr. Draffin added that the plan, with the approval of OAG, is for the fellow to focus on the cybersecurity needs of public water service providers. A report with recommendations would be useful to the PSC as it continues to include cybersecurity in its regulation of covered utilities. In response to these comments, Senator Hester commended Mr. Draffin, Mr. Abeles, and Ms. Hayes for their work during the session on SB 800/HB 969.

Subcommittee on Education and Workforce Development. Senator Hester focused her subcommittee report on SB 801/HB 1189 (Economic Development – Cybersecurity – Cyber Maryland Program) which she and Delegate Forbes proposed. She noted that

In essence, the bill implements the US Chamber’s Talent Pipeline Management Model for expanding the state’s cyber workforce. Central to the model is inviting industry with education and training providers to define the skills needed, to develop the training programs to provide those skills, and as practicable, to target training on groups traditionally underrepresented in cybersecurity. She pointed out that the bill assigns administrative responsibility for the program to TEDCO, establishes a CyberMaryland Advisory Board charged with creating a strategic plan, and creates a CyberMaryland Fund from which to support training and education efforts.

The Senator observed that it took four years to shape a bill that could pass, and she commended the subcommittee for its contributions over the years that led to the successful 2023 bill.

Subcommittee on Economic Development. Ms. Leong-hong observed that the new Administration has brought a strong focus on innovation, creating a climate that will favor business expansion in the state. There are challenges, of course. She mentioned that VC capital is harder to come by. But within the state, she noted that TEDCO has a number of initiatives underway to support start-ups. She asked if any of her subcommittee members had anything to add in the way of observations from their last meeting. In response, Mr. Israel concurred that VC is much more difficult to raise. Consequently, businesses are looking for alternatives, such as how to use SBIs or how to access resources provided by TEDCO. Ms. Leong-hong concluded by noting that the subcommittee would focus on crafting recommendations to support start-ups and an economy of innovation in the state.

Subcommittee on Public and Community Outreach. Ms. Rogan mentioned that the subcommittee had been meeting as a working group to devise and then launch a survey of Maryland adults to gauge their level of cybersecurity awareness. The funding for this survey was provided by Johns Hopkins University and the National Cryptologic Foundation. The preliminary results were presented and discussed at the subcommittee’s public meeting on May 19. Ms. Rogan asked Dr. Dahbura, a member of her subcommittee, to provide an overview.

Dr. Dahbura observed that over 400 adults had responded to the survey which was conducted on Mechanical Turk. He cautioned that the findings suggested further research and should not be treated inferentially valid for the general adult population of the state. He made five major points about the findings:

Respondents were overconfident in their cybersecurity knowledge

There were high reported victim rates for online scams

Password reuse was practiced by more than 30% of the respondents

Respondents exhibited a lack of awareness that their personally identifiable information had likely been compromised.

He concluded his presentation by noting that the findings will be used to inform future TT1t3 (nfor)6 binarQq0 t

TT1t3 (nfor)6 binarQ q 0 t1vp (s)]* n98.16 W* n d(a)4 (a likend)6 ng th.6sucudors pePompromised.

Mr. Petersen drew attention to