Draft 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, Brian Israel, Dr. Anupam Joshi, Mary Kane, Miheer Khona, Mathew Lee, Bel Leong-hong, Kimberly Mentzell, Laura Nelson, Steve Pennington, Rodney Petersen, Jonathan Powell, Sue Rogan, and Troy Stoval.

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

Acting Chair's Welcome

Mr. Kemerer welcomed the Council members and guests on behalf of Attorney General Brown who was not able to chair the meeting due to his schedule. Mr. Kemerer noted that he and Dr. von Lehmen had the opportunity to brief the Attorney General on the Council in May and that the Attorney General hopes to chair the fall plenary meeting. Mr. Kemerer thanked the University of Maryland Global Campus for its hospitality in hosting the meeting.

Subject Matter Expert Presentation

After reviewing the agenda, Mr. Kemerer introduced the guest presenter, Mr. Mathew Scholl, Chief, Computer Security Division, National Institute for Standards and Technology (NIST). Mr. Scholl's presentation focused on the threat of quantum computing to cryptography and NIST's competition to develop quantum proof encryption. Mr. Scholl's presentation included the following key points:

- The next 2 to 15 years will bring major technological disruption. This will come as a result of major emerging technologies, quantum and AI. Quantum is a category that includes quantum information science, quantum mathematics, quantum engineering, and quantum computing.
- Quantum computing has moved from a theoretical question to a practical engineering challenge. The machines seen in the media are efforts to prove out the technology so that quantum machines can be built at scale. The goal is quantum supremacy, which describes machines that can perform better than current computing technology. Machines that will

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. Without such a process, there will not be trust in the solutions by the commercial or government sectors, and this will be a barrier to adoption. The response to the NIST challenge was worldwide with 69 candidate algorithms from 25 countries.
- NIST set out several criteria for these solutions. They must only be strong but also must be simple, resistant to many ways of attack, and implementable within the existing digital infrastructure. Through a series of testing rounds, most of the submissions failed for one reason or another and were removed from the competition. The primary two that NIST has endorsed are "Crystals" and "Kiber and Crystals". There is also a third, Dilithium. The goal is to have a pool of algorithms based on different mathematical foundations so that if some are later broken resiliency is offered by a pool of alternatives.
- NIST's goal is to finalize a standard by early 2024 so that industry can then begin to develop and market the solutions. Big companies are already moving: Google, Microsoft, Amazon, Samsung, and Cisco. Migrations at scale have been difficult for enterprises to do. Consequently, NIST is also working with industry and government to develop tools that will help enterprises with the migration to a new standard of encryption.
- The big question is when will quantum computing be deployed at scale and when does quantum-proof encryption need to be implemented. The Federal government has set 2035 as the target for its transition to be complete. This deadline will have a big pull on the private sector, since the encryption requirements will apply to the many contractors working with the government.
- Quantum will spawn many other scientific advances that have been held back by the lack of capacity for complex modeling, such as drug research, weather modelling, and many areas of physics. It is important the US be at the forefront of these efforts. To this end, there is the Quantum Economic Development Consortium, an open group that aims to build out the quantum engineering infrastructure of the US.

In response to the presentation, there were a number of questions.

Senator Hester asked what advice Mr. Scholl would give state governments as they grapple with the necessity of migrating to quantum-proof solutions to protect their data. His advice is to ensure that software product vendors have a plan for cryptographic modernization and updates for the future so that the government is not locked into a specific implementation that will require it to do an implementation all over again. Vendor claims about the quantum resistant character of their products need to be peeled back and carefully examined.

Dr. von Lehmen asked how much visibility the US has into the quantum-proof encryption efforts of adversary nations like China and also whether there was any reaction to Bruce Schneier's blog post about the reliability of NIST's algorithm screening effort. Mr. Scholl answered that the Chinese adopted an early round submission to NIST, tweaked it, made it the PRC standard, and launched a lobbying effort to get other nations to adopt that standard. It sought a first mover advantage. That effort failed since its standard lacks transparency. It is not clear what the tweaks

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 provided the subcommittee report on behalf of Mr. Levin who was not able to attend. He noted that the subcommittee's February meeting was dedicated to a discussion of the Council's Ad Hoc Subcommittee on Consumer and Child and the then-forthcoming SB 698/HB 807 that the ad hoc subcommittee informed. The bill was proposed by Delegate Love and Senator Augustine in lieu of Susan Lee who had chaired the ad hoc subcommittee but left the General Assembly before the 2023 session began.

Mr. Feldman pointed out that the ad hoc subcommittee benefitted from numerous stakeholder presentations over five meetings and commended Michael Lori for recruiting those presenters. While SB 698/HB 807 did not make it out of committee, Mr. Feldman stated that he expected a similar bill would be proposed next year. He expressed the gratitude of his subcommittee members for Susan Lee's leadership on cyber-related consumer protection issues during her years on the Council and in the General Assembly.

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 this is bill, which was enacted in the last session, will significantly advance cyber workforce development in the state. She underscored that bill was informed by extensive fact-finding within her Council subcommittee that included presentations by representatives of the US Chamber of Commerce, the Kentucky Chamber of Commerce, Cyber Florida, and the Georgia Cyber Center.

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 webinar programming by the subcommittee and that a goal is to conduct a follow-up survey by engaging an experienced survey research organization.

In response to the presentation, Senator Hester stated that there should be a policy response to data like this, such as an aggressive state PSA campaign to raise awareness.

Mr. Petersen drew attention to the national cyber awareness and education program at NIST. He previewed that likely in July there will be a new national cyber workforce and education strategy. The first pillar will focus on foundational cyber skills for all Americans. There will likely be e a push from the White House and at the national level in this connection. He also mentioned that NIST, the National Cybersecurity Alliance, and CISA have a multi factor authentication Campaign that has been running for the last couple of years. But what is really needed is for states and governors to join that campaign and use some of the videos, messaging, and materials NIST has already put together. It is difficult for the federal government to scale the use of these materials, especially at the K 12 level since control falls under state and local control.

Other business

Mr. Kemerer asked Dr. von Lehmen to provide an update on the biennial report due to the General Assembly no later than July 1. Dr. Von Lehmen reminded that the report had been distributed to the Council for comment and thanked the members who had reviewed the draft. He asked that all comments be provided by June 19th.

Lt Col Ferguson noted that Adjutant General Janeen Birckhead was unable to join because of other duties and asked for a moment to update on the activities of the Maryland National Guard. He noted that:

- The Guard had developed and exercised and incident response plan for the state.
- the National Guard Bureau released a capability called NITRO, which is a resilient timing source for networks. Maryland is one of the first 5 States to join.
- The Guard has begun to leverage DoD's innovative readiness training program in Maryland. The purpose of the program is to uses military capability to improve civilian affairs

Adjournment

Mr. Kemerer asked if there was other business. Hearing none, the meeting was adjourned at 2:04 pm on motions made by Ms. Kane and Ms. Leong-hong.