Minutes
Maryland Cybersecurity Council Meeting
October 17, 2019
10:00 am – 12:00 pm
Chesapeake Room
College Park Marriott Hotel and Conference Center
At University of Maryland Global Campus
Hyattsville, Maryland

Council Members Present or Represented (33/57)
Mr. Donald Fry (for Attorney General Brian Frosh, Chair), Dr. David Anyiwo, Delegate Ned Carey, Dr. Michel Cukier, Robert Day, Chas Eby (for Russell Strickland), Judi Emmel, Mary Jo Hayes, Senator Katie Fry Hester, Fred Hoover, Clay House, Brian Israel, Dr. Anupam Joshi, Yessim Karaman (for Walter Landon), Dr. Kevin Kornegay (for Dr. David Wilson), Secretary Michael Leahy, Senator Susan Lee, Delegate Mary Ann Lisanti, Bel Leong-hong, Ken McCreedy, Joseph Morales, Colonel Reid Novotny (for MG Timothy Gowan), Colonel William Pallozzi, Jonathan Powell, Jonathan Prutow, Markus Rauschecker, Christine Ross, Danielle Santos (for Donna Dodson), Gregg Smith, Stacy Smith, Paul Tiao, Steven Tiller, and Pegeen Townsend.

Staff Attending
Patrice Drago (Chief of Staff, Office of Delegate Carey), Howard Barr (Assistant Attorney General and Principal Counsel, DoIT), Steve Sakamoto-Wengel (Office of the Attorney General, Consumer Protection Counsel for Regulation, Legislation and Policy), and Dr. Greg von Lehmen (Council Staff, UMUC).

Subject Matter Expert Presenter
Mr. Frank Grimmelmann, President and CEO, Arizona Cyber Threat Response Alliance (ACTRA)

Council Meeting

<u>Opening Remarks by the Chair</u>
Mr. Donald Fry chaired the meeting on behalf of the Attorney General who was unable to participate. In his opening remarks, Mr. Fry:

- Called for a moment of silence for Representative Elijah Cummings whose passing that had been announced earlier in the morning.
- Welcomed new members to the Council: Senator Katie Fry Hester (District 9) as the new chair of the Education and Workforce Development Subcommittee, Dr. Michel Cukier for the University of Maryland, Mr. Gregg Smith for CAMI, and Ms. Stacey Smith in her new role at the Maryland Tech Council.

- Expressed appreciation on behalf of the Attorney General to Dr. Ken McCreedy for his service to the Council and to the State. Mr. Fry announced that Dr. McCreedy would be retiring from his position as Director of Cybersecurity and Aerospace at the Maryland Department of Commerce.

Call for the Minutes

The chair observed that the Council had received the minutes of its 22 May 2019 meeting in advance. He asked for any amendments. Hearing none, the minutes were approved on motions duly made and seconded.

Council Updates

The chair reminded the Council that its next meeting will be in January and that staff were working with both the AG's office and the potential speaker on a date that will be announced soon.

Subcommittee Reports.

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee.

The subcommittee met on October 02 and invited stakeholders to provide feedback on bills it has been considering. Senator's Lee's comments included the following:

- Maryland Consumer Protection Act (2019 SB 613/HB 901). This bill is modelled on the California Consumer Protection Act (CCPA). However, the bill will be modified to benefit from the evolution of the law in California and to address as much as possible the specific concerns that stakeholders have been voicing to the subcommittee. The invitation to provide input remains open, and the subcommittee looks forward to working with all interested parties to shape a bill that avoids unanticipated consequences.

- Security Features for Connected Devices (SB 553/HB 1276). The bill will provide a regulatory framework for IoT devices in Maryland. The security requirements would apply to all IoT devices sold in the State. Subject to certain provisos, the bill would require public bodies to purchase devices that meet the bill's requirements. The Attorney General would be able to seek relief. The bill provides no private right of action.

- Updates to MPIPA. The basis of the updates are the relevant provisions of 2019 SB 786/HB 1127 (Financial Consumer Protection Act) which was not voted on in committee during the last session. The bill is in the process of being modified to take into account comments that the subcommittee has received.

- Ransomware Bill (2019 HB 211). The bill would update the computer intrusion law to raise the penalties for such intrusions and to include hospitals within the bill's coverage. The bill makes knowing possession of ransomware with an intent to harm a misdemeanor and makes intrusion a felony. The bill does not apply to ransomware that is used purely for research purposes. It permits a right of private action.

- Bill to expand the role of the State Department of Information Technology is overseeing cybersecurity policy for public entities within Maryland. The bill under discussion within the subcommittee is based on the 2018 North Dakota Bill 2110.

Secretary Michael Leahy, Chair, Cyber Operations and Incident Response Subcommittee

The Secretary provided an update on activities by the Department of Information Technology (DoIT). He noted that DoIT has caught up on patching systems and was launching a vulnerability management initiative that goes beyond the specific reaction to the ransomware threat to broadly protecting systems. Finally, he noted that the subcommittee would meet soon to standardize DoIT's handbook and to ensure its alignment with the Governor's most recent executive order.

Markus Rauschecker, Chair, Critical Infrastructure Subcommittee

- A representative of the Emergency Numbers Systems Board (ENSB) made a presentation at the subcommittee's September 13 meeting. The objective was to inform the subcommittee of the State's transition to digital 911 service, the board's efforts to create standards to help ensure the cybersecurity of the new system, and to explore how the subcommittee or the full Council might assist the board. This initial consultation was pursuant to 2019 SB 339 (Public Safety – 911 Emergency Telephone System) which requires that the ENSB to develop standards in consultation with the Council.

  In addition, the subcommittee continued its discussions about:

- How an Information Sharing and Analysis Organization (ISAO) could be created and sustained in Maryland. The members looked forward to the presentation by Mr. Frank Grimmelmann to inform the subcommittee's discussion.

- Outreach to the utility sector to assess what regulatory or statutory changes might support enhanced cybersecurity for the sector. The objective is to avoid a top-down approach and to start with the industry members themselves. Dr. von Lehmen committed to the subcommittee to seek additional staff resources in consultation with OAG to support this initiative. Specifically, he will apply for an NSA Fellow to be assigned to OAG for the purpose of doing CI research.

- Adding new resources to the repository.

Bel Leong-hong, Chair, Economic Development Subcommittee.

Ms. Leong-hong noted that the subcommittee's September 24 planning meeting was a consequential one, committing the subcommittee to focusing on two of its recommendations in the July 1, 2019 Activities Report:

Recommendation 6 (Support for IP start-ups). The subcommittee recognizes the need, noted in the EXCEL Maryland report and other places, to find ways to accelerate the transition from lab to market for new cybersecurity products. The processes at the universities for doing this are complicated. TEDCO cannot do it all alone. Other entities in the cyber ecology have successful track records in supporting IP startups that bear examination. What other states are doing is informative too. Georgia, for example, has created a cyber innovation zone with appropriate incentives to attract investment in the commercialization of cyber-related IP. Since Maryland already has innovation zones, it might consider linking them, so that they work together as a network. Members of the subcommittee will engage with the business community to explore specific approaches that the subcommittee could shape into actionable recommendations.

Recommendation 7 (Streamlining tax credit related to cybersecurity). Based on feedback from the business community, the subcommittee believes that the 'buy Maryland' tax credit is difficult for businesses to qualify for and therefore is underutilized. The member of the subcommittee from the Maryland Department of Commerce (Ken McCreedy) agreed to convene a group of stakeholders to see what changes could be proposed.

Ms. Leong-hong observed that her subcommittee would like to partner with the Education and Workforce Development Subcommittee on her subcommittee's Recommendation 5 (Cybersecurity Workforce Development). Recommendation 5 seeks to expand cybersecurity apprenticeship programs by providing additional incentives to employers. Ms. Leong-hong also mentioned her subcommittee's ongoing concern about security clearance process. It continues to be a major problem for firms wanting to bid on government contracts or trying to fulfill contracts already won.

In response to Ms. Leong-hong's report:

- Senator Lee indicated that the Law, Policy and Legislation Subcommittee would be willing to work with the Economic Development Subcommittee on the tech transfer issue. The Senator agreed that looking at what has worked in other states would be very useful.
- Brian Israel pointed to the successful work of DataTribe in facilitating commercialization of technology out of Ft. Meade and recommended including them in the discussion.
- Mr. Fry acknowledged how the critical nature of the security clearance issue but observed that it is a federal problem that there is little that can be done by state government to remedy it.

Senator Katie Fry Hester, Chair, Subcommittee on Education and Workforce Development

Senator Hester introduced herself to the Council, indicating how excited she was to chair the subcommittee. She noted that she is co-chair of the General Assembly's Joint Committee on Cybersecurity, Technology and Biotechnology and that she saw some intersection between the concerns of the Council in general, her subcommittee in particular, and the Joint Committee.

The subcommittee held an organizational meeting on October 10. This enabled the Senator and one other new member—Dr. Michel—to meet the other members and to consider what issues or concerns the subcommittee should focus on in the next two years. The Senator noted that a number of ideas were advanced, such as the need for more State investment in public university computer science and cybersecurity departments, and how such a recommendation might be supported by a report that would baseline Maryland against other state university systems.

The Senator indicated that the subcommittee would convene for a longer meeting in the near future to dive more deeply into the cyber-related workforce development issues in the State. She expressed the thought that it might be helpful to explore these issues in the next hearing of the Joint Committee on December 4. She pointed out that since the next legislative session is likely to look carefully at the Kirwan Commission recommendations, the context is there for looking at workforce development issues.

Dr. Greg von Lehmen for Ms. Sue Rogan, Chair, Public And Community Outreach Subcommittee

Dr. von Lehmen conveyed Ms. Rogan's regrets for having a conflict that precluded her for participating in the Council's meeting. He noted that the subcommittee members were continuing to suggest resources to the repository in partnership with the Critical Infrastructure subcommittee.

<u>Subject Matter Expert Presentation</u>

Mr. Fry welcomed Mr. Grimmelmann to the Council and thanked the University of Maryland Global Campus for financially supporting Mr. Grimmelamnn's visit to Maryland.

To establish context for the presentation, Mr. Fry noted that the need for an Information Sharing and Analysis Organization (ISAO) in Maryland for small and medium-size businesses has been a topic of discussion within at least two of the Council's subcommittees and has been the vision of Dr. McCreedy and others in State government. Efforts have been made to realize the vision, but for various reasons, they have not yet been able to bear fruit.

Mr. Grimmelmann expressed his gratitude for the invitation and indicated that his comments about ACTRA would address five points: 1) what ACTRA is and its underlying philosophy, 2) how it began, 3) how it is organized, 4) how it fits within the larger landscape of information sharing, and 5) what its sustaining business model is.

Key points from his presentation included the following:

- There is no 'one size fits all" when it comes to ISAOs.
- ACTRA is a grass-roots driven 503 (c3) organization. It is overseen by a 13-member board of directors. The founding membership included five companies in Arizona. Today, it has a broad membership with a primary focus on about 300 companies identified as critical infrastructure by DHS. It acts as a trusted bridge between the private sector and law enforcement, fusion centers and other government entities.
- ACTRA grew out of the Arizona InfraGard. It was launched in 2013 as part of an effort to figure out how to get actionable information about cyber threats quickly. The top-down approach to information sharing causes delays. ACTRA is based on a team-of-teams approach. It leverages the advantages offered by federal partners while relying on a wide ground-level peer network within which each member is willing to share information about the threats it is seeing and how it is responding. This enables faster sharing of threat information and faster speed of reaction. ACTRA is a coalition of the willing protecting themselves through the power of their network.
- Consequently, ACTRA's value proposition to the private sector is threefold. It offers firms: a) strong perimeter defense through peer-to-peer information exchange, b) information superiority, and c) threat intelligence that is operationalized and actionable.
- ACTRA works on all levels to enhance the capabilities of its members and the power of the network. These efforts map to culture, workforce development, and technology. One example of this is ACTRA's Cyber Academy. It is an apprenticeship program across all 16 critical infrastructure sectors. Another is ACTRA effort to create a network of cyber ranges that includes government, education, healthcare, and other critical infrastructure companies to develop an environment for innovation.

In response to Mr. Grimmelmann's presentation, several Council members raised questions:
Mr. Paul Tiao: To its credit, DHS has established a program of regional Cybersecurity Advisors (CSAs) to assist state and local entities. What is the level of maturity of this program? Secondly, did the Cybersecurity Information Sharing Act of 2015 galvanize the creation of ISAOs?
Mr. Grimmelmann: Regions should work with their CSAs. They can provide valuable information about resources and access to Washington where needed. To the second question: CISA to date has not sparked the rapid formation of ISAOs across the country.

Mr. Markus Rauschecker: how could Maryland get a something like ACTRA off the ground?
Mr. Grimmelman: ACTRA took an entrepreneurial approach. The answer is the value proposition for private companies that attracted their willingness to help. Needed is an initial funding source. They bootstrapped the organization on an initial grant of about $300,000 from an energy company, built capacity and brought operations online later. Sustainability requires affordability. Today, membership within ACTRA is $4,500/year.

Mr. Steve Tiller: Could you give specific examples of how the information sharing worked?
Mr. Grimmelmann: One example is the WannaCry ransomware attack. ACTRA has a number of Fortune 500 companies whose Arizona offices have operations around the world. ACTRA was notified within hours after one company's London office experienced the WannaCry attack. A

notification to ACTRA members went out quickly and was followed with updated advisories, indicators of compromise (IOCs), and strategies for defense.

Senator Lee observed that Maryland has suffered its share of ransomware attacks and would have benefitted from an ACTRA-like organization. She noted that combatting threats is a multiprong effort that includes empowering legal action against unlawful intruders and raising the penalties for ransomware and other attacks.

Mr. Clay House: How did the engagement model work when ACTRA was establishing itself and what is the typical timeline.
Mr. Grimmelmann: There is no "typical"; everyone is different. They come from a different place, have different maturity levels, and have different priorities. They start with an assessment and go from there. It usually takes about a year. ACTRA's model is not to make money on its engagements but to expand the community.

With no other questions from the floor, Mr. Fry thanked Mr. Grimmelmann for his presentation.

Other Business and Adjournment

There being no further business, Mr. Fry adjourned the Council at 12:00 pm.