Minutes
Maryland Cybersecurity Council Meeting
June 13, 2018
10:00 am – 12:00 pm
College Park Marriott Hotel and Conference Center
At University of Maryland University College
Hyattsville, Maryland

Council Members Present or Represented (30/57)
Attorney General Brian Frosh (Chair), John Abeles, Kevin Crain (for Kristin Jones Bryce), Dr. Anton Dahbura, Robert Day, Cyril Draffin, Judi Emmel, Howard Feldman, Don Fry, Zack Fry (for Pete Landon), Clay House, Brian Israel, Dr. Anupam Joshi, Miheer Khona, Mathew Lee, Blair Levin, Fred Hoover, Senator Susan Lee, Anthony Lisuzzo, Rajan Natarajan, Mark Miraglia (for Ken McCreedy), Jonathan Powell, Markus Rauschecker (for Professor Greenberger), Sue Rogan, Christine Ross, Senator Bryan Simonaire, Lance Schine (for Secretary Michael Leahy), Stacey Smith, Pegeen Townsend, and Clarence Williams.

Staff Attending
Tiffany Harvey (Chief Counsel, Legislative Affairs, OAG), Howard Barr (Principal Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Susan Lee), Linda Wilk (NSA Fellow, Maryland Department of Commerce), Dr. Frederick Ferrer (MCAC), Dr. Greg von Lehmen (Council Staff, UMUC).

Subject Matter Expert Presenter
Bill Lawrence, Director, E-ISAC and Senior Director, North American Reliability Corporation

Council Meeting

Opening Remarks by the Chair

The Attorney General welcomed the members and expressed his appreciation for their commitment to the Council's work. Regarding the last session, he thanked both the legislative members who had sponsored bills aligned in principle with the Council's recommendations and other members who had testified for those bills.

He introduced several new members to the Council: Linda Lamone (Administrator, State Board of Elections), Fred Hoover (Senior Program Director, National Association of State Energy Officials), Clarence Williams (Lead for Government Engagement, NICE), and Patrick Feehan (Information Services and Privacy Director, Montgomery College).

He updated the Council on its letter to the Governor calling for significantly increased funding to secure the state's networks. The letter was acknowledged, and its timing was opportune. It coincided with the formation of a working group under the Governor's cybersecurity executive order. The group submitted a report to the Governor on June 1. The Attorney General observed that the security of the state's systems needs major attention. While the Governor may not be able to share the report due to its sensitivity, the Council was able to provide informed input at a critical time.

Before turning to the subcommittee reports and the presentation by Mr. Lawrence, the Attorney General called for the minutes. Motions to approve were made and seconded, and there being no objections, the minutes were approved.

Subcommittee Reports

Senator Susan Lee, Co-chair, Law, Policy and Legislation Subcommittee, for both her and Mr. Blair Levin.

On behalf of herself and Blair Levin, Senator Lee thanked the members of the subcommittee for their contributions in the last session and their efforts to prepare for the next. She noted that the subcommittee had met on June 5. She concurred with the Attorney General's assessment that the 2018 session saw a number of bills pass that were consistent with the Council's recommendations:

- SB 202/HB 710 (Credit Report Security Freezes). Senator Lee, Delegate Carey and Delegate Lisanti. Extending legislation passed in 2017, the bill requires that credit reporting companies like Equifax provide consumers affected by a breach with free credit freezes and thaws of their credit reports without limit.

- HB 281 (Securing the Future: Cybersecurity Education for All). Delegate Aruna Miller. The bill requires that beginning with the 2021/2022 school year, each public high school must offer at least one computer science course and school districts must make efforts to incorporate computer science in elementary and middle schools too. The bill calls for increasing enrollments of traditionally underrepresented groups in computer science. It also establishes the Maryland Center for Computing Education at the University System of Maryland to engage in activities to strengthen the skills and increase the number of computer science teachers.

- SB 228 (Cybersecurity Investment Tax Credit). Senator Guzzone. The bill has three components covering convertible debt and the 'buy Maryland' tax incentive in addition to the investor tax credit. The credit is structures so that 75% of the tax credits shall be awarded for purchase of cyber products to encourage development of IP.

Senator Lee noted that there were bills that did not move in this session:

- SB 376/HB 456 (Cyber Intrusion and Ransomware). Senator Lee and Delegate Barron. Even though the bill was similar to statutes in other states, it did not move out of committee because it thought that while ransomware is a new threat, its effects are already provided for by the extortion law and other parts of the state code. With the Council, the subcommittee strongly believes that given ransomware's diverse uses—from simple extortion to disruption of operations—and its potential for catastrophic impact, including loss of life, it should be specifically called out as a crime in a bill with appropriate penalties.

- SB 882 (Telecommunications and Computer Network Access). Senator Lee. The bill would have enforced net neutrality of ISPs by making it a requirement of any ISP doing business with the state government and would have set standards for the procurement of IoT devices by the state. Cyril Draffin, a member of the Critical Infrastructure Subcommittee, provided helpful testimony on IoT and the complexity of securing it.

The Senator concluded by outlining the subcommittee's program of work for the next session:

- Draft revised ransomware bill. Two approaches are being discussed. These include incorporating ransomware in computer intrusion legislation and ala Michigan Public Act 95, making possession of ransomware per se illegal with appropriate carveouts (e.g. protecting ransomware research).
- Draft a bill requiring ISPs to obtain affirmative consumer consent before sharing browser history. This may be a first step toward a similar requirement that would apply more broadly to data brokers.
- Draft amendment to MPIPA to add geolocation and perhaps other attributes to the class of PII protected by the statute.
- Draft updates to state breach law to align it with changes in MPIPA.

She noted that the subcommittee had decided to defer action on standards for state IoT procurements, pending a forthcoming NIST special report, and that it may ask the Council to adopt a formal recommendation endorsing net neutrality.

Mr. Israel asked how large the Maryland teacher shortage in computer science is in cybersecurity and what the state was doing to address it. Senator Lee answered that there is a significant shortage and that HB 281 seeks to address it through the Maryland Center for Computing Education housed at USM.

Dr. Joshi concurred that the new Center will be an important vehicle for all of the universities within the system to contribute to professional teacher training in computer science and cybersecurity. In this connection, he mentioned the Business Higher Education Foundation case study of cybersecurity education within USM that highlighted the degree programs at College

Park, UMBC, Towson, UMUC, and Bowie State. (The case study, Building a Diverse Talent Ecosystem in Cybersecurity, can be found online at http://www.bhef.com/publications.)

Lance Schine, Deputy DoIT Secretary, for Secretary Michael Leahy, Chair, Incident Response Subcommittee

Mr. Schine indicated that there are no updates for the subcommittee.

Mr. Markus Rauschecker for Professor Michael Greenberger, Chair, Critical Infrastructure Subcommittee

Mr. Rauschecker conveyed Professor Greenberger's regrets for not being able to join the meeting and offered three updates that he had discussed with him:

- The Council's online cybersecurity repository. To contribute to the depth and currency of the new repository, the subcommittee has made significant progress is compiling a second installment of resources for small- and medium-size entities. John Abeles had suggested hundreds of additions. His efforts and those of other subcommittee members are being supplemented by student research assistants at the University of Maryland Francis King Carey School of Law. The goal is to add these resources to the repository before the next full Council meeting on October 16.

- Information sharing entity for Maryland (Joint recommendation of the Critical Infrastructure and Cyber Operations and Incident Response Subcommittees). Active discussions involving GOHS and DoIT are underway to form such an entity. The Critical Infrastructure Subcommittee has been connected to these discussions via Linda Wilk who has been providing research support for the state effort. Among the inputs it has provided, the subcommittee shared a draft plan for an information sharing organization drafted by one of its members (Clay Wilson). The state's work on an information sharing entity had started with Chuck Ames, former Cybersecurity Director for DoIT and delegate for Secretary Leahy on the Cyber Operations and Incident Response Subcommittee.

- Possible legislation to address CI owner needs. The subcommittee plans to undertake a program of direct outreach to infrastructure owners in Maryland to better understand their challenges. This information will shape subcommittee recommendations to support efforts by critical infrastructure owners to enhance their cybersecurity.

Senator Simonaire for Professor Jonathan Katz, Chair, Education and Workforce Development Subcommittee

The Senator observed that one of the recommendations of the subcommittee was a scholarship for service program for Maryland that would be based on the National Science Foundation model. In consultation with Dr. Katz, he and Senator Lee successfully proposed such a program in the last session (SB 204). Aimed at full-time cybersecurity students the program requires that

scholarship recipients in two-year, four year or master's programs provide one year of service to the state government for every year of scholarship support. The Governor has allocated $150,000 for the first year of the program.

Beyond recommendations made by the Council, the Senator noted two other legislative initiatives related to cybersecurity that he sponsored or co-sponsored. SB 281 (Maryland Cybersecurity Council - Membership – Revisions**)** added the Administrator of the State Board of Elections to the Council. SB 553 (State Government - Security Training - Protection of Security-Sensitive Data) requires the state to identify employees who handle "security sensitive data" and provide annual security overview training or refresher training for these employees.

Dr. von Lehmen commented that MHEC administers a large scholarship budget and asked whether any of those funds would be reprogrammed for cybersecurity scholarships. Senator Simonaire stated that those funds are dedicated for specific purposes by statute and cannot be reprogrammed for cybersecurity.

Sue Rogan, chair, Subcommittee on Public and Community Outreach

Ms. Rogan had three updates for the Council informed by the subcommittee's meeting on May 21.

- Resources for the repository. While the Critical Infrastructure Subcommittee is compiling resources helpful to small and medium-size organizations, her subcommittee is identifying resources that would be of use to the general consumer. These concern best practices about how to operate safely online as an individual. Like the Critical Infrastructure Subcommittee, her subcommittee is aims to submit these resources prior to the Council's October 16 meeting.

- Support for an event. As part of its outreach mission, the subcommittee will seek support from the Attorney General's Office for the Council to serve as a sponsor to an educational event targeting small- and medium size businesses.

- SB 202/HB 710 (Credit Report Security Freezes). The new law is a major incentive for consumers to protect themselves with a credit freeze. The subcommittee will look for opportunities to inform the general public, whether through webinars or other platforms.

Ms. Stacey Smith for Ms. Bel Leong-hong, Chair, Subcommittee on Economic Development

Ms. Smith mentioned that Ms. Leong-hong regretted that she could not be present. In preparation for the Council meeting, however, Ms. Leong-hong had convened the subcommittee on June 11, which agreed to the following report-out.

Ms. Smith observed that the subcommittee's recommendations in *the July 2017 Activities Report* were broad. In general, the subcommittee was asked to consider additional proposals to support

the development and growth of the cyber-related business sector in Maryland in concert with other initiatives. These included but were not limited to a substitute package for the Investment Tax Credit, income tax and other incentives to give Maryland an edge in recruiting skilled professionals into the state, and incentives for firms to take on student interns to accelerate their security clearance process. The bills that members of the subcommittee supported in the last session and plan for the next are consistent with the Council's 2017 charge. Specifically,

- SB 228 (Cybersecurity Investment Tax Credit). Ms. Smith noted that a key contribution of subcommittee members and other organizations was the amendment to the bill that recognized convertible debt as a form of financing. This extended the tax credit to this particular investment vehicle and multiplied the incentive for investment in cybersecurity start-ups in Maryland.

- SB 517/HB 1226 (Career Apprenticeship Investment Act). This bill, which did not pass in the last session, aims in part to establish matching grants to expand apprenticeship opportunities in workforce shortage areas and hard-to-fill local government jobs, including those in cybersecurity. Maryland like every state faces a workforce shortage in cybersecurity, felt acutely by government entities. The subcommittee anticipates that this bill will be proposed in 2019, and subcommittee members will be supporting it as aligned with the broad charge in the *2017 Activities Report*.

- Income tax credit for cybersecurity professionals locating to Maryland to accept a position. Mentioned above as part of the 2017 recommendations of the Council, this tax credit continues to be discussed within the subcommittee. Other states are offering such incentives, and the subcommittee believes it is worth discussing with the Council's legislative delegation whether such a bill should be proposed in 2019.

- 2017 HB 873 (Income Tax Credit – Security Clearances – Employer Costs – Extension). Sponsored by Delegate Carey, this bill extended the tax credit that firms could claim against the cost of meeting security requirements (e.g. building a SCIF). It appears to be the case that only large firms have the administrative capacity to take advantage of this credit, and the subcommittee has discussed the possibility of suggesting an amendment that would create a care-out for smaller firms.

- State tax credit for start-ups against payroll. Such a credit would recognize the fact that start-ups do not generate net revenue in the near-term, but they do have payroll and must pay payroll taxes. The federal government recognizes this by permitting start-ups a credit against their payroll taxes. The subcommittee believes that Maryland should do the same.

- Guardian angels for start-ups. The subcommittee is considering formal proposals that would provide incentives for large firms and academic institutions to partner with start-ups to allow them to pilot their products and services. This might be especially appropriate for universities that have spawned start-ups.

- Accelerating security clearances. A major obstacle in filling positions by Maryland firms serving the federal government is the requirement for a clearance. This is because a) the time to obtain a clearance is well over a year and b) the process cannot start until the individual needing a clearance is hired. Members of the subcommittee and their organizations—Christine Ross (Maryland Chamber of Commerce) and Tamie Howie (Maryland Tech Council)—have been at the forefront of the effort to engage federal agencies about ways to speed the clearance process. They have broached the idea of using internships and apprenticeships as on-ramps for the clearance process. These efforts may be superseded by announced changes in responsibility for clearances from OPM to DoD. It is reported that DoD will bring efficiencies to the process, reducing the time needed.

- Safe harbor for firms implementing recognized cybersecurity standards. The State of Ohio in its 2017-2018 session passed a bill (201SB 220) that incentivizes firms to invest in cybersecurity standards by allowing those firms to use the investment as an affirmative defense when they are sued as a result of a breach. The subcommittee will discuss proposing such a bill with the legislative delegation of the Council.

Ms. Smith concluded her report by noting that the subcommittee's members hope to collaborate with members of other subcommittees on the foregoing and with other organizations in the state.

Mr. Israel remarked that SB 228, particularly the tax credits for convertible debt and 'buying local', will significantly enhance the state's ability to attract cybersecurity firms to locate in Maryland. Ms. Smith added that the bill is a first nationally, was given attention by Senator Cardin on the Senate Committee on Small Business and Entrepreneurship and has resulted in inquiries from a number of other states.

Subject Matter Expert Presentation

The Attorney General welcomed Mr. Bill Lawrence and thanked Mr. Draffin for recruiting him to speak. Mr. Lawrence expressed his appreciation for the invitation. He noted that he is a Maryland resident and is pleased to be able to assist the Council by giving an overview of the electric grid, the e-ISAC, and what is being done to ensure the grid's resiliency.

Mr. Lawrence's presentation (PowerPoint) covered the following points:

- E-ISAC History
- Mission and Vision
- North America's Grid
- Threat landscape and common threats
- Information sharing and examples
- Products, services, and other resources
- International attacks
- GridEx opportunities and lessons learned

Key take-aways from the presentation:

- The E-ISAC is one of the founding ISACs responsive to President Clinton's Presidential Directive 63. Since 1999, it has been housed at the North American Electric Reliability Corporation (NERC). NERC creates and enforces mandatory standards for the bulk generation and transmission of electricity across the North America. Distribution is regulated at the state level. Because of NERC Critical Infrastructure Protection (CIP) Standards, the grid starts from a baseline of security that is almost unique among the critical infrastructure sectors. The nuclear power sector also has mandatory and enforceable standards.

- The E-ISAC's mission is to reduce cyber and physical security risk to the electricity industry across the US (including Hawaii and Alaska), Canada and Mexico. This mission extends to bulk generation, transmission *and* distribution of electricity. Its vision is to provide high quality analysis and rapid information sharing for utilities and to help stakeholders mature their capacity to deflect, manage, and recover from adverse events. The E-ISAC analytical capacities are enhanced by its partnerships with the federal government, state organizations, and national laboratories funded by DoE and DHS.

- The threats to the grid range from damage caused by animals, weather (wind, lightning), theft (copper components for resale), or simple accidents to the most extreme possibilities of EMP or nuclear war. More recently, cyber threats (e.g. ransomware) and terrorist activity (e.g. disabling transformers through gunfire) have been added to the list. In this area, the E-ISAC focuses on two domains: information technology (IT)—the enterprise networks that utilities rely on to run their business and technical operations—and operations technology (OT), the physical components of the grid—like industrial control devices—that are run through the networks.

- The E-ISAC offers a variety of products and services to the industry, some of which come with reciprocal responsibilities. It supplies subject matter and context to NERC alerts which may require the industry to provide information addressing questions that bear on the alert itself. In an emergency, NERC can issue the highest-level NERC alert (not used to date), which can direct utilities to take certain operational actions to protect and restore the grid. The E-ISAC issues reports, provides resources, and socializes best practices such as the NIST Cybersecurity Framework and the Energy Subsector Cybersecurity Coordination and Maturity model (C2M2).

- A critical service of the E-ISAC is organizing the GridEx every two years. These exercises build response capabilities among utilities and related stakeholders, including state and local governments. Each GridEx last two days, are massive, and engage participants in complex, extremely challenging scenarios involving both IT and OT related attacks. Participation in these exercises has been growing. For example, the 2017 GridEx involved 6,500 participants, 450 organizations including 206 utilities, and 14 states. Two states, Wisconsin and South Carolina used the 2017 GridEx to meet their full-scale emergency management training exercise for the year, with their National Guards and emergency management agencies

participating. These exercises include a table-top piece to engage executives about strategy and policy. In 2017, Dr. Mary Beth Tung from the Maryland Energy Administration participated in that exercise. These exercises generate lessons learned and agreements. One of the outcomes of the 2015 GridEx is a mutual assistance agreement among 140 utilities to assist each other in the event of a massive cyber attack.

- The E-ISAC benefits from international partnerships. A case in point are the attacks on the Ukrainian power grid in 2015 and 2016. With some sources attributing the attacks to Russia, the 2015 attack involved remote access of control room computers to turn off the breakers, interrupting power. A DDoS attack prevented phone calls to the utilities to slow their awareness of the situation and to cause panic among callers not able to get through. However, once aware, the utilities dispatched teams to the field to manually reset breakers. The result was a quarter of a million people without power for only 8 hours. A similar attack on the transmission of electricity in 2016 affected 100,000 people for just a few hours. E-ISAC and other US agencies have debriefed extensively with the Ukrainian companies and passed these lessons learned on to their stakeholders.

- The disaggregated nature of the electric utility industry and the complexity it creates is a defensive strength of the US system. The network architecture of each utility company differs from one to another, as do their physical systems. To penetrate a substantial part of the industry would require huge investment of time and resources to map the networks and physical equipment of each utility. In addition, there are manual work-arounds when systems are taken down. The grid as a whole is not invulnerable, but its complexity raises the challenge significantly for any adversary contemplating a broad cyber attack against the American infrastructure.

In response to Mr. Lawrence's presentation, the following members raised questions:

- Dr. Tony Dahbura: How common is it for members of the E-ISAC to find advanced persistent threats (APTs) in their systems? Mr. Lawrence: APTs are found from time to time. The reports about Russia targeting the energy sector is a case in point. To help identify these campaigns, NERC and E-ISAC administer the Cybersecurity Risk Information Sharing Program (CRISP). Under CRISP, member utilities share data on traffic entering and leaving their networks, forming the largest repository of critical infrastructure data in the world. This traffic is analyzed by the E-ISAC and shared through classified channels for evaluation at the DOE level, which can access intelligence from the CIA, NSA, and the FBI. Site specific information is provided back to utilities where a threat is identified. The indicators of compromise (IoCs) are published to the entire industry.

- Dr. Joshi: First, can the E-ISAC share its GridEx attack scenarios with academic institutions to use in their degree programs? Second, can E-ISAC discuss the separation between networks and OT systems? Mr. Lawrence: It is on the E-ISAC roadmap to share more with academic institutions. In regard to the second question, the CIP standards require the absolute separation of networks for administrative traffic, like email, and networks connected to OT. This is in addition to other protections—both electronic and physical—that are mandated.

- Mr. Hoover. Does IoT—smart meters as an example—offer a vector at the distribution level for cyber threats? Mr. Lawrence: The answer is yes. The E-ISAC is very much aware of this threat. To start addressing it, DOE is working with states like New York and California on initiatives to require that security be baked into these devices. At a more general level, the E-ISAC is working on faster ways to share information that is more like DHS Automated Indicator Sharing (AIS) system.

- Mr. Abeles: Energy security is top-of-mind right now for DOE. Recently, there have been at least three or four reports that have been published by the department in this connection. Is E-ISAC connected with DOE's efforts to secure the nation's energy? Mr. Lawrence: The DOE is the sector-specific agency that NERC and E-ISAC interact with, and they are very much involved with its efforts.

- Mr. Rauschecker: In regard to the CIP standards, are there penalties for noncompliance and how significant are those penalties? Mr. Lawrence: To broaden the question, NERC has a range of standards in addition to the CIP. These other standards include grid operation, incident response, facility engineering, and more. Penalties for violations can be as high as $1 million per day. In 2011, when there was a blackout in the Southwest, it was found that the utilities responsible were not following NERC standards. The penalties assigned ranged from $7 million to $16 million. The goal now is to move beyond compliance as a mentality to viewing the standards as a foundation on which utilities can build more security. He has seen that shift accelerate in his time with E-ISAC.

- Dr. von Lehmen: Does NERC or DOE or DHS have a general communication plan in the event the grid goes down nationally for a sustained period of time? How would the government communicate with the general public to provide updates and direction? Without communication, a sustained outage is likely to produce deep social chaos. Mr. Lawrence: An outage as described is extremely unlikely. There is a supplemental operations strategy under which the utilities would operate the grid manually if necessary to restore power. To ensure their ability to coordinate a response, the utility sector is looking at ways independent of the normal networks to communicate among themselves and with government partners, such as satellite phones and high-frequency radios. The use of these devices will be built into the next GridEx. But to the question: preparing to manage a sustained general power outage, including the ability to communicate with the general citizenry, really must start at the state and local level. The experience with hurricanes in Florida and Texas demonstrate that.

- Dr. von Lehmen: We've heard about serious security breaches in the last few years. In these cases, very advanced cyber weapons in our national arsenal have been stolen. Breaches of CIA's Vault 8 and NSA's Equation Group are examples. When classified tools are known to be in the hands of adversaries or criminal groups, are utilities notified in a particular way about the risks so that they can be prepared? Mr. Lawrence: It surely happens at some level. The E-ISAC through DoE has relationships with all of the key law enforcement and intelligence agencies. There is a challenge in the ability to shared classified information because not everyone is cleared. But on the other hand, the CRISP program allows threat information to be declassified and shared within 24 to 36 hours.

- Attorney General Frosh: Could you explain again how Wisconsin and South Carolina used GridEx? Mr. Lawrence: These states have used the exercise to roll out their entire suite of government functions---emergency management, fusion centers, and the National Guard—to work with utilities, NERC, and other federal agencies to manage the scenarios thrown at them. This not only builds experience but also establishes relationships that can be called upon in an actual crisis.

There being no other questions, the Attorney General thanked Mr. Lawrence for an excellent presentation and for his willingness to entertain questions.

Other Business and Adjournment

The Attorney General asked if there was any new business. Hearing none, he reminded the Council of the October 16, 2018, meeting at UMUC and adjourned the members at 11:35 am.

Minutes approved without objection by the Council on October 16, 2018, as recorded by Council staff.