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

Council Members Attending
Greg Garcia (Chair), Senator Susan Lee (for Chairman Mike Miller), Senator Bryan Simonaire, Senator Katherine Klausmeier (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 Wilkinson (NSA Red, 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 W R &RXQFLO ¶V Regarding the last session, he thanked both the legislative members who had sponsored bills aligned in principle Z L W K &RXQFLO ¶ V U H F R P P H Q G D W 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 Manager, [illegible] and Clarence Williams (Leahan (Information Services and Privacy Director, Montgomery College).

He updated the Council on its letter to the Governor calling for significantly increased funding to

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

scholarship recipients in two-year, four year or graduate programs to 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 she sponsored or co-sponsored. SB 281 (Maryland Cybersecurity Council - Membership and Revisions) added the Administrator of the State Board of

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 VHVVLRQ DQG SODQ IRU WKH QH[W DUH Specifically, WHQ Z L W K

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 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 WKH VXEFRPPLWWHH EHOLHYHV LW LV ZRUWK GLVFXVVL 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)[2] 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 (2018 SB 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 by reporting that she hopes 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 bonds and loans, 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 its security.

Mr. Lawrence's presentation (Power

Mr. 54bB86 -1d(wha)f 98and

Key take-aways from the presentation:

- The E-ISAC is one of the outgrowths of 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 American grid. 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 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

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

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- , 6 $ & F R Q Q H F W H G Z L W K ' 2 (¶ V H I I R U W V W R V H F X U H W K H 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.

' U Y R Q / H K P H Q : H ¶ Y H K H D U G D E R X W V H U L R X V V H F X U L W \ cases, very advanced cyber weapons in our national arsenal have been stolen. Breaches of & , $ ¶ V 9 D X O W 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[2] 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 ca