

Summary
Maryland Cybersecurity Council Meeting
October 18, 2016

Mr. Fry then turned to the subcommittee chair reports. He noted that in its *July 2016 Interim Activities Report*, the Council had identified many initiatives that were prioritized after review by the Attorney General and in discussions with the subcommittee chairs. Mr. Fry noted that the *Report* is a public document that can be found online. The subcommittee reports are summarized below.

Senator Susan Lee, Subcommittee for Law, Policy and Legislation

Cyber First Responder Reserve. The subcommittee continues to accumulate information to shape the concept of a reserve. This information includes the activity of the National Guard's cyber units and the existence of the Maryland Defense Force that works with the Guard. It also has included discussions with MEMA.

MEMA has noted that its role in relation to a cyber first responder group would be the same as it is now with respect to other groups involved in an emergency response, namely MEMA would be the coordinating agency, not the lead agency. DoIT would be the lead agency in an incident response. DoIT is actively working on a full incident response plan and MEMA is participating in that effort and will share the plan with the subcommittee. When a first responder group is activated, it must be integrated into the plan.

Other points pertinent to establishing the cyber first responders reserve.

If the emergency involved private critical infrastructure, there would need to be coordination with the private sector, since the State does not have direct control of private entities.

The State does not have a list of specific public and private infrastructure entities falling with the 16 US DHS critical infrastructure categories.

If a first responder reserve is authorized and formed, MEMA will need additional funding to manage or coordinate it. Now 75% of MEMA's funding is from the federal government.

MEMA and DoIT have exercised a cyber emergency (table top) but more exercises will follow to identify gaps in communication, coordination, equipment and technical talent to refine the plan and better prepare for its execution.

Markus Rauschecker for Michael Greenberger, Chair, Critical Infrastructure Committee.

Mr. Rauschecker indicated that due to other business Professor Greenberger was not able to participate in the Council meeting and conveyed his regrets. He identified three lines of effort by the subcommittee:

The first is to establish an educational infrastructure that provides resources (information on issues, frameworks, standards, best practices, threat sharing mechanisms) to Maryland critical infrastructure sectors and other stakeholders in the State. Mr. Rauschecker noted that there are many resources available through the federal government, the State of Maryland and a variety of other entities. The challenge is that there is no one place where they are catalogued and easily accessible. This is particularly a problem for small and medium-size entities that do not have large dedicated cybersecurity teams. The recommendation would help address this challenge. Mr. Rauschecker indicated that other subcommittees were looking at the same issue and that developing a portal of some type would be a collaborative effort.

The second is to identify the critical infrastructure sectors that are at greatest risk of cyber attacks and need the most enhanced cybersecurity measures. The US Department of Homeland Security of course has identified 16 critical infrastructure (CI) sectors, but the State could benefit from a better inventory of its CI infrastructure and which sectors need more support. This effort would also recognize the interdependencies among sectors, including geographical interdependencies. For example, every sector is dependent on the electrical grid and Maryland's power can be affected by interruptions in other states.

The third is to encourage critical infrastructure and other private sector entities to conduct risk assessments and to provide information concerning resources and tools to help entities conduct risk assessments. Most critical infrastructure is in private hands, although there are some, like water

Dr. von Lehmen indicated that the Attorney General had approved three subcommittee recommendations for action and provided the update below on their status:

Assess cyber workforce demands in Maryland. The aim of this initiative is to help inform educational programs in cybersecurity to keep pace with changing needs. The subcommittee has paused its effort in this area because the recommendation may be achieved by a project funded by NIST through the National Initiative of Cybersecurity Education (NICE). The purpose of the project is to compile current and granular information about the cybersecurity job requirements that employers are looking to fill in every state and locality. The first iteration of the data will be available on the web and previewed at the NICE Annual conference in November. The subcommittee will assess whether the data achieves its goal.

Develop a scholarship for state service proposal. The subcommittee believes that such a program might help State agencies with their workforce needs in cybersecurity. It has collected information about the federal scholarship for service program and is currently considering how Maryland might be able to fund a similar program for Maryland.

Support K-12 computer science pipeline-building efforts. The subcommittee has just begun work on this recommendation. It is aware that MSDE is making significant strides in this area and has obtained the support of a liaison to help the subcommittee understand the full range of the Department's pipeline building efforts before developing proposals that MSDE might welcome.

Dr. von Lehmen was asked about the status of computer science training in K-12, and he mentioned the Career and Technical Education (CTE) programs in this area that are offered by public high schools. But he noted that a challenge is finding teachers who can offer computer science courses. Another member of the Council pointed out that the University of Maryland, College Park, is working with the State under an NSF grant to train computer science teachers. Other comments were that computer science is considered 'shop'—and not science—in schools creating a disincentive for students to take the courses and that well-equipped labs as well as trained teachers is a challenge.

Bel Leong-Hong, Chair, Subcommittee on Economic Development

Ms. Leong-Hong noted that the charter of the subcommittee is to find ways to attract, grow and retain cyber-related businesses in Maryland. There are three recommendations that the subcommittee has organized around:

Map the lifecycle of a technology-oriented firm. The subcommittee has identified several models with the idea of understanding the needs of these firms at each stage in their development.

Development of an asset map for Maryland. The objective is to comprehensively identify what resources the State offers for cyber-related firms and how these resources map from start-up through maturity.

Incentives to support the growth of the State's cyb

clearance tax credit, and a one-time income tax credit to attract cybersecurity professionals to Maryland.

Sue Rogan, Chair, Public Awareness and Community Outreach

Ms. Rogan was the final chair to report out. She updated the Council on the cybersecurity repository the subcommittee is creating and hopes to launch by July 1, 2017. There are many collections of information on cybersecurity covering a vast range of topics. The subcommittee's goal is to create one web-based portal where these other resources can be collected and catalogued for easy use. This project may link to initiatives of other subcommittees which aim to create libraries of resources for specific audiences. The Maryland Department of Information

with the message that developing the talent needed by the Guard and civil society requires teaching young people the importance of personal responsibility, leadership and ethics. The Maryland National Guard is very active in answering invitations to go into schools to talk about these things. The Guard is working to expand its outreach program by involving its retirees.

Mr. Fry expressed the Council's appreciation to Colonel Bratton for a very substantive presentation and to Major General Singh both for making him available and for her remarks. There being no further business on the agenda, on behalf of Attorney General Frosh Mr. Fry again thanked the Council, its contributors, and the staff for their work.

Meeting adjourned at noon.