Meeting Minutes

Maryland Cybersecurity Council
Subcommittee on Critical Infrastructure
Friday, September 13, 2019
11:00 am – 1:00 pm
Marriott Inn and Conference Center at UMUC
3501 University Boulevard East
Hyattsville, Maryland

Attendance (7/13)

Subcommittee members attending: Markus Rauschecker (chair), John Abeles, David Anyiwo, Cyril Draffin, Terri Jo Hayes, Fred Hoover, and Colonel Reid Novotny (for MG Linda Singh).

Staff: Howard Barr (Assistant Attorney General and Principal Counsel, DoIT) and Dr. Greg von Lehmen (Staff, Maryland Cybersecurity Council)

Meeting Summary

1. The chair welcomed the members and framed the purpose of the meeting: to identify broad recommendations to be included in the Council's 2019 Activities Report as a roadmap for committee work through 2021.
2. The minutes for the October 11, 2018, meeting of the committee were unanimously approved.
3. Proposed recommendations for the upcoming Activities Report:

The resource database. The repository on the Council's website has grown as a result of recommendations of the CI subcommittee and other Council subcommittees. A new collection of resources will be added by the next full Council meeting in May. Recommendation: as the database expands, the subcommittee should review the search tools, tagging and descriptions of the resources to ensure ease of use by businesses and consumers.

Risk assessment and policy recommendations. Mindful of its statutory charge, the committee identified the categories of critical infrastructure which in principle have the greatest possibility of catastrophic consequences for the state. These are energy, banking/finance, communications, healthcare, transportation, and information technology. In the 2019 – 2021 period the committee will focus on the utility sector to assess both the vulnerability of providers and to formulate recommendations supportive of enhanced cybersecurity within that sector. Committee due diligence will include meetings with CI owners and government regulators, among other methods such as the use of the C2M2 tool.

Information sharing. The committee recommends the establishment of an information sharing entity to be nested at the University System of Maryland level that would provide local awareness of cyber threats to Maryland critical infrastructure providers and government agencies and offer a variety of other services, such as training. It is conceived that this entity would be led by full-time, appropriate qualified professionals but staffed by undergraduate and graduate students providing a service to the state and job experience to students. Organizationally, the entity would be established on the model of Maryland Center for Computing Education (MCCE) created by 2017 HB 281 and would be funded by the state.

General level of CI cybersecurity. The committee recommends legislation that would incentivize businesses across the 16 DHS CI sectors within the state to implement the NIST CsF, CIS controls, ISO, or some other nationally recognized standard.

There being no other business, the meeting was adjourned at 1:15 pm.