Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Law, Policy and Legislation
Thursday, October 11, 2018
2:30 pm – 3:30 pm
UMUC Administration Building
Room 1001
3501 University Boulevard East
Hyattsville, Maryland

Attendance

Subcommittee members attending: Senator Susan Lee, Blair Levin, Patrice Drago (Chief of Staff for Delegate Ned Carey), Howard Feldman, Joseph Morales, Jonathan Prutow, Markus Rauschecker (for Professor Michael Greenberger), and Paul Tiao. (Quorum present 8/9)

Staff: Howard Barr (Assistant Attorney General and General Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Lee), and Dr. Greg von Lehmen (Staff, Maryland Cybersecurity Council).

Members of the public: Kevin Callahan (CompTia), Ariel Fox Johnson (Commonsense.org), Shum Preston (Commonsense.org), Katie McGinnis (Consumer Reports), Salena Musuta (Mozilla Fellow at Consumer Reports), and Carl Szabo (NetChoice).

Meeting Summary

1. Welcome by Senator Lee who announced that a quorum of the subcommittee was present. She provided an opportunity for representatives of organizations who came to the meeting to introduce themselves.
2. Call for the minutes of the June 5, 2018, meeting of the subcommittee. The minutes were approved by the members.
3. Discussion of new business:

a) California Consumer Protection Act (SB 1121). Ms. Ariel Fox Johnson (Commonsense.org) briefed the subcommittee on the most current version of the statute. Questions and discussion followed.

b) Safe harbor. This discussion focused on Ohio 2017 SB 220 as a possible model for Maryland. Howard Feldman noted that safe harbor offering an affirmative defense in the case of a breach will not deter plaintiff's attorney from suit to obtain a settlement. Better would be a presumption that a standard of care had been met in the case of firms that implement a recognized cybersecurity standard. Paul Tiao drew the subcommittee's attention to the federal SAFETY Act as a potential model for encouraging businesses to implement a recognized security standard. The act provides certain liability protections for entities that have received a designation or certification from the Department of Homeland Security for the sale or provision of "qualified anti-terrorism technology" to customers.

c) Ransomware. Michael Lore explained the work with the legislative committee on this issue. He drew attention to a Michigan statute on the subject and also a compilation of ransomware attacks on state and local government entities and whether ransom was paid.

d) Net neutrality. Articles in the media have commented on the cybersecurity implications of net neutrality. Mr. Levin drew attention of the subcommittee to the recent DoJ suit filed against California in which the Department argues that net neutrality issue has been preempted by federal action. A concern is that the Court could hand down a decision that is too broad and could wipe away state laws on cybersecurity issues. His recommendation is that Maryland should weigh into the legal action on the side of California in order to protect the progress that states have made in the area of cybersecurity.

e) Internet of Things (IoT). The subcommittee discussed California's SB 327. The law requires manufacturers to take reasonable steps to secure IoT devices defined as those that have IP addresses and communicate via Bluetooth. These steps include unique default passwords and offering consumers the option of changing passwords.

f) Algorithms used to determine credit and consumer access to other services. Michael Lore distributed an article and briefed the subcommittee on the issue.

4. Given the subcommittee's interest in the foregoing, Senator Lee will brief out the discussion of the subcommittee for the consideration of the full Council at its October 16 meeting.

5. The meeting was adjourned at 11:20 pm.