Meeting Minutes
Maryland Cybersecurity Council
Subcommittee on Law, Policy, and Legislation
Friday, October 9, 2020
1:00 pm – 2:30 pm
Virtual Meeting

Attendance (Quorum Present, 8/9)
Subcommittee members attending: Senator Susan Lee and Blair Levin (co-chairs), Patrice Drago for Delegate Ned Carey, Howard Feldman, Joseph Morales, Markus Rauschecker (for Professor Michael Greenberger), Paul Tiao, and Pegeen Townsend.

Staff: Hanna Abrams (Assistant Attorney General, Consumer Protection Division), Howard Barr (Assistant Attorney General and General Counsel, DoIT), Michael Lore (Chief of Staff, Office of Senator Lee), Steve Sakamoto-Wendel (Consumer Protection Counsel for Regulation, Legislation and Policy, Consumer Protection Division) and Dr. Greg von Lehmen (Staff, Maryland Cybersecurity Council).

Members of the public: Chris DiPietro, Jenna Masson, Caitlin McDonough, Bernie Marczyk, Ellen Valentino.

Meeting Summary

1. Chairing and opening the meeting, Senator Lee thanked all for their attendance.
2. A quorum was announced. Minutes of the 02 October 2019 were called for and approved unanimously on motions made and seconded.
3. Senator Lee noted that the 2020 legislative session was challenging because it was ended in March. The General Assembly was not able to consider all bills. The budget was the priority. No bills related to cybersecurity were passed by both chambers. It has not been announced when members of the General Assembly will go in in January.
4. Given the outcomes of the 2020 session, she will propose the cybersecurity bills again in January. She hoped that the subcommittee meeting would restart discussion of those bills with all interested parties to ensure that the bills consider all points of view.

2019 SB 120 (State Government – Department of Information Technology – Cybersecurity

Senator Lee noted that SB 120 passed the House in 2020 but did not emerge from committee in the Senate. The bills is similar to one enacted in North Dakota and was recommended by the last State CISO, John Evans. With COVID, and the shift to remote working and online education, the bill is even more important in the assistance it would offer.

2020 Fiscal Policy Note Summary of the bill
SB 120 expands the responsibilities of the Secretary of Information Technology to include (1) advising and consulting with the Legislative and Judicial branches of State government regarding a cybersecurity strategy and (2) in consultation with the Attorney General, advising and overseeing a consistent cybersecurity strategy for units of State government, including institutions under the control of the governing boards of the public institutions of

higher education, counties, municipal corporations, school districts, and all other political subdivisions of the State

2020 SB 201/HB 237 (Commercial Law – Personal Information Protection Act – Revisions).

Senator Lee indicated that she thought the bill could pass in 2021. It is consistent with legislation that the General Assembly has already passed and merely updates the definition of personal information in response to advances in technology.

Hanna Abrams pointed out that there was greater public understanding of geolocation as a result of contact tracing. She asked whether the bill's inclusion of social media should be removed. Patrice Drago noted that both geolocation and social media had been removed from the definition of personal information last session in the discussions with interested parties.

Howard Feldman pointed to a practical problem with the Section §14–3501 (e)(i)(1) of the current PIPA statute, suggesting that unencrypted names should not be considered "personal information in the meaning of the statute". This would require a change in the law:

From:
(e) *(1)* "Personal Information means:

(i) An individual's first name or first initial and last name in combination with any one **or** more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable"

To

(i) "An individual's first name or first initial and last name in combination with any one or more of the following data elements, *when the data elements* are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable"

Michael Lore agreed with the change and suggested that the current language was a drafting error that could be rectified.

2020 Fiscal Policy Note Summary of the bill
SB 201/HB 237 expands the Maryland Personal Information Protection Act (MPIPA) by (1) covering additional types of personal information; (2) expanding the types of businesses that are required to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized use; (3) shortening the period within which businesses must provide required notifications to consumers after a data breach; and (4) requiring additional information to be provided to the Office of the Attorney General (OAG) after a breach has occurred. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

2020 SB 443 Consumer Protection – Security Features for Connected Devices

Michael Lore noted that the bill is consistent with FTC guidelines.

Paul Tiao asked whether the bill covered industrial control devices as well as consumer products, whether there was grandfathering of products already on the market, and whether enforcement action would fall on the seller or the manufacturer. Michael Lore observed that the bill only pertains to consumer products, not to industrial control devices. Senator Lee noted that enforcement action would fall on the manufacturer, not on the seller.

Mr. Tiao indicated that the bill would not only extend some protection to the consumer but might also diminish botnets and have larger social benefits. Given that California enacted a similar law, Mr. Tiao suggested that it would be beneficial to know their experience with it.

Senator Lee observed, as did Patrice Drago for Delegate Carey, that the Senate and House committee members last session did not understand the need for the bill. Both thought it would be useful to arrange a demonstration of how easy it is to hack IoT devices. Dr. von Lehmen was asked to explore whether that could be done.

2020 Fiscal Policy Note Summary of the bill
SB 443 requires a manufacturer of a "connected device" to equip the device with a reasonable "security feature" that is (1) appropriate to the nature and function of the connected device; (2) appropriate to the information the connected device collects, contains, or transmits; and (3) designed to protect the connected device from unauthorized access, destruction , or modification. A connected device is considered to have a reasonable security feature if it meets these requirements and is equipped with a means for authentication outside of a local area network that includes either (1) a preprogrammed password that is unique to each connected device or (2) a process that requires the user to generate a new means of authentication before the user is granted access for the first time. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

SB 30/HB 215 (Criminal Law – Crimes Involving Computers – Ransomware)

Senator Lee observed that the surge in ransomware attacks this year makes the bill more important than ever and thought that it had a high probability of passing. In the last session, the bill was heard but the session ended before it could be voted out.

Mr. Tiao pointed out that the context has changed dramatically. A few years back ransomware was not a major problem. Today it is with big ransoms being demanded. The most common vector is business email compromise.

2020 Fiscal Policy Note Summary
This bill prohibits a person from knowingly possessing "ransomware" with the intent to use it for specified purposes and establishes criminal penalties for violations. The bill applies prospectively to any cause of action arising on or after the bill's October 1, 2020 effective date.

2020 SB 957 (Maryland Online Consumer Protection Act (MCPA)

Senator Lee emphasized that she would like to get input regarding changes to the bill from all interested parties. Michael Lore observed that the discussion that had begun last session was very helpful. He hoped to pick up where they had left off. Every input is important. He would like to have more feedback from the clients of lobbyists about what is concerning about the bill, why, and ideas about how those concerns could be met.

2020 Fiscal Policy Note Summary
This bill establishes numerous personal information privacy rights for consumers in the State. Specifically, the bill establishes for consumers the right to (1) know whether (and what) personal information is collected or disclosed by a business; (2) access (and obtain a copy of) personal information collected by a business; (3) have personal information deleted by a business; (4) stop a business from disclosing information to third parties; and (5) equal service and pricing, regardless of whether the consumer has exercised his or her rights under the bill. Violation of the bill is an unfair, abusive, or deceptive trade practice under the Maryland Consumer Protection Act (MCPA), subject to MCPA's civil and criminal penalty provisions.

5. Hearing no further business, Senator Lee asked for motions to adjourn. Meeting adjourned at 2:00 pm.

[Note: These minutes were approved by the subcommittee at its 01 June 2021 meeting.]