Date: February 24, 2020
Time: 10:00am - 11:00am
Location: 100 Community Place, Crownsville, Maryland 21032

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Maryland Cybersecurity Coordinating Council

Meeting Minutes

Council Member Attendance:

Council Member	Title	Organization	Status
Charles “Chip” Stewart	SCISO	DoIT	Present
Walter "Pete" Landon	Director	GoHS	Represented by Mark Hubbard
David Brinkley	Secretary	DBM	Absent
Ellington Churchill	Secretary	DGS	Represented by Eric Lomboy
Lourdes Padilla	Secretary	DHS	Absent
Robert Green	Secretary	DPSCS	Represented by Kevin Combs
Robert Neall	Secretary	MDH	Present
Timothy Gowen	Adjutant General	DMIL	Absent
Russell Strickland	Director	MEMA	Represented by Chas Eby
Woodrow Jones	Superintendent	MSP	Absent
Gregory Slater	Secretary	MDOT	Represented by Jeffrey Hirsch

Call to Order: Chip Stewart, 10:03am
(Roll Call taken, and noted above)

Review Meeting Minutes from August 8, 2019 and November 7, 2020
Motion: Approve meeting minutes from the previous two Maryland Cybersecurity Coordinating Council quarterly meetings.
Yea- 7

Stewart: Minutes will be posted shortly

Current Cybersecurity Climate:
Stewart: In today's meeting we will be discussing the current cybersecurity climate. Cryptomining and ransomware are two things that we are seeing. If council members see value in a demonstration on ransomware, Chip Stewart would like to use a personal laptop and initiate a ransomware attack to show viewers the process in action.

Overview of Ransomware:
Ransomware attacks generally utilize a standard set of steps, known as a "kill-chain". These begin with a reconnaissance phase, where the hacker builds a profile of his/her intended target. From this information, the hacker chooses a specific person or entity and attacks. The method of attack may vary and may include installing a payload or manually installing ransomware through servers. Once a system has been infiltrated, any larger systems that are linked to it may become vulnerable.

Increasing Ransomware Attacks:
Cybersecurity attacks against state and local governments have increased throughout the years. These numbers are just the ones that were reported. There is probably underreporting, but this shows the trend.
2013 - 2 attacks
2014 - 3 attacks
2015 -6 attacks
2016 -54 attacks
2017 - 46 attacks
2018 - 58 attacks - 169 attacks total over the course of 6 years. As of 2018, the most expensive recovery from a cybersecurity attack is $17 million, against the City of Atlanta.
2019 - 114 attacks...More than two attacks a week.
The first month of 2020 is at 17 that we know of.

Stewart: The nature of cybersecurity attacks has changed. Previously, efforts were made to restore backups when an attacker infiltrated a system. Now, hackers are threatening to release data if they do not receive payment.

Neall: It looks likes Utah has escaped attacks [referring to PowerPoint slide]
Stewart: It is possible that attacks from Utah have not been recorded or perhaps their process is working. [then moving to a different slide] It looks like Utah was attacked in 2019.

Stewart: Functionally, what does this mean for our state agencies? How do we respond when a cybersecurity attack happens? The question is not *if* the cybersecurity incident happens but *when*….

Stewart: Currently, there are substantial issues with systems connected to the State's network. Moving forward, the security operations center will be contacting your agencies much more. When DoIT hears about third-party vulnerabilities, the council members will be notified.

Audience member: Where does this information come from?
Stewart: We receive notices from federal partners, and utilize open-source intelligence.
Audience member: Is someone else running their own scans and providing you with the results?
Stewart: Yes, [in other words] these are the IP addresses you have and this is what you are seeing ....[these numbers include] universities, libraries, counties. The information provides an interesting perspective and is both encouraging and discouraging. The State has room to improve, but this information shows that we are not the easiest target.

Hirsch: Are you seeing attacks against ICS systems?
Stewart: We are starting to see ransomware attacks involving Industrial Control Systems and SCADA systems. Attackers have discovered that the value of those systems is higher and so they will attack those.

Audience Member: What lessons can we take away from Baltimore City?
Stewart: I would like to think that many of the lessons that were learned do not apply to DoIT; some the patches missing in Baltimore were completely below standards. One lesson DoIT did take away from the Baltimore attack is about remote desktop exposure--this provided the attackers with an easy way in and an opportunity to establish a beach-head.

National Governors Association (NGA) Event:
A number of MCCC council members attended the NGA event that took place at the beginning of the new year. Attendees included:

- GoHS
- MCAC
- MEMA
- MDNG
- DoIT

NGA Workshop goals included:

- Determining the State's strategy in response to a cybersecurity incident.
- Refining and implementing the statewide Cyber-Disruption Plan
    - By the end of 2020, DoIT hopes to send out a draft for review

Was this workshop a success?
Stewart: The State was afforded an opportunity to test the Cyber-Disruption Plan last month. Cannot be happier with how it played out.

Eby: Very happy with how the NGA event went and would be happy to participate/plan another session. It has been interesting to see the work between the counties and the State. We have to continue to leverage relationships between them. In the past, this has been a barrier.
Stewart: Yes, relationships are key. The State has a high level of trust with many of the counties.

Outreach to State Agencies:
The goal is to update and review the State of Maryland Information Technology Security Manual in July 2020. If there are any changes to suggest, please contact Chip Stewart directly at chip.stewart@maryland.gov.

A few noticeable areas that require attention...

- ATO/C&A Process
    - This is too vague and requires clarification (e.g., Who needs to do what? What does "unsupported" mean?)
- Incident Reporting
    - What defines something as "bad?" Who do you report to? How is a report submitted?

We hope to have feedback submitted in a week or two. If we receive substantial feedback, DoIT will consider incorporating it into the existing draft(s). If we do not hear back, DoIT will proceed with publishing the official policies to the DoIT website.

DoIT has been working more with the FBI--this is considered a huge win. The FBI trusts the State and, in the recent event that we previously mentioned, the FBI agreed to split the evidence collection for the incident.

New Business:
Eby: Wanted to highlight Senate Bill 1036. MEMA is closely watching this bill, which would create a cybersecurity coordination unit within MEMA. It is not so technical but focused more on planning and training. MEMA is also in the process of hiring planning staff who can work with cyber disruption planning. There is synergy and this is something MCCC council members should be aware of.

Hubbard: In May, we will be talking about all things cyber. Chip Stewart can obtain an agenda through Mark Hubbard or Blake Langford.
Stewart: More than happy to attend, if it is appropriate.

Stewart: The next MCCC meeting should be in late April. Soft copies of the policies will be emailed and the deadline for comments regarding the policies will be included.

Closing Proposed Motion - Vote to Conclude, 10:43am
Moved- Chas Eby
Second- Jeff Hirsh
Yea- All
Nay-

Abstain-

Chairman of Board APPROVAL  Date: 11/4/2020