Date: November 7, 2019
Time: 10:00am - 11:30am
Location: 100 Community Place, Crownsville, Maryland 21032

Maryland

**DEPARTMENT OF
INFORMATION TECHNOLOGY**

Maryland Cybersecurity Coordinating Council
Meeting Minutes

Council Members in Attendance

- Charles "Chip" Stewart, State Chief Information Security Officer (DoIT)
- General Adam Flasch, designee for General Gowen Adjutant General, Military Department (MIL)
- Kevin Combs, designee for Secretary Green, Department of Public Safety and Correctional Services (DPSCS)
- Russell Strickland, Executive Director, Maryland Emergency Management Agency (MEMA)
- Walter "Pete" Landon, Director, Governor's Office of Homeland Security (GOHS)
- William Pallozzi, Superintendent, Maryland State Police(MSP)
- Robert Neall, Secretary, Maryland Department of Health (MDH)

Council Members Not Present

- Lourdes Padilla, Secretary, Department of Human Services (DHS)
- Pete Rahn, Secretary, Maryland Department of Transportation(MDOT)
- Ellington Churchill, Secretary, Department of General Services (DGS)
- David Brinkley, Secretary, Department of Budget & Management (DBM)

Call to Order: Chip Stewart, 10:00am

The meeting began with the mention of new Maryland Cybersecurity Coordinating Council members. The two new members are General Timothy Gowen and Mr. Charles "Chip" Stewart. General Gowen was not in attendance but sent a designee. Chip Stewart introduced himself as Maryland's new State Chief Information Security Officer.

Review Meeting Minutes from August 8, 2019

Incident Reporting - Chip Stewart

Chip reviewed the Incident Reporting slide. The information he reviewed is as follows:
Incidents include events that impact, or have the potential to impact, any of the following:
- The availability of a system or data
- The confidentiality of non-public state data
- The private PII of one or more individuals
- The integrity of a system or data
- The disclosure of credentials used to access a State system or system with State data

DoIT will send a memo to all agencies about incident reporting.

Question (Jitendra Chandna - DHS): What is the reporting process?
Chip Stewart: Incidents should be reported to the SOC...Chip can send information after the meeting. The policy is already in place and detail will be provided shortly, with further guidance coming out sometime in the next few months

State of Maryland Information Technology Security Manual:
In June, a new State of Maryland Information Technology Security Manual was released. This new manual was a full rewrite of the previous edition. The goal was to present a new manual quickly, to replace the previous, outdated policy. Since its release, new challenges have been discovered, such as establishing clear definitions for otherwise vague words. An example of this is in describing some software as "unsupported."

DoIT is working with the National Governors Association (NGA) to clarify terms, and requirements, to continue improving the current security manual.

DoIT is also striving for substantial improvements to security, in reference to credential stuffing. Credential stuffing increases the chance that an important system is compromised. When an unimportant system is compromised, it can compromise an important system that shares the same account credentials (e.g., passwords).

> **Chip Stewart**: Credential stuffing--the practice of using the same account credentials for many applications/systems--is becoming more common and makes a party, or parties, more vulnerable to attack.

To prevent this vulnerability from being exploited, DoIT hopes to establish a secure single sign-on portal as a standard for agencies. Eventually, this will be required for all applications.

Flasch: Inquired whether there would still be a username and password.
Stewart: Responded that we hope to use that single identity provider in combination with hardware keys ... probably Yubikey.

Supply Chain Risk Management- Chip Stewart

Recently, some states have experienced attacks that were propagated from a third party/vendor. Many products are advertised as secure products, and most procurements require a SOC 2 Type 2 audit report. DoIT and DBM offer support on the Procurement and Evaluation side for these vendor-provided reports.

Russell Strickland: Regarding RAM, when does DoIT want input?

Chip Stewart: DoIT would like the input to be iterative; the goal is to constantly improve. Ongoing input will help with progress...One of the ways DoIT hopes to improve is by offering a DoIT-supported software library. Currently, we do not have a list of approved software, but we hope to establish this.

Vote to Conclude Public Session

Moved- Chip Stewart

Second- William Pallozzi

Yea- Bob Neall, Kevin Combs, and Adam Flasch

Nay-

Abstain-

Chairman of Board APPROVAL _Charles I Stewart III_ Date: _3/2/2020_