Date: January 28, 2021
Time: 9:00am - 10:00am
Location: Virtual

Maryland Cybersecurity Coordinating Council

Meeting Minutes

Call to Order, Chip Stewart: 9:01am

Roll Call:

Council Member Attendance:

Council Member	Title	Organization	Status
Charles "Chip" Stewart	SCISO & Chairman	DoIT	Present
Walter "Pete" Landon	Director	GoHS	Present
David Brinkley	Secretary	DBM	Represented by Derek Mitchell
Ellington Churchill	Secretary	DGS	Represented by Eric Lomboy
Lourdes Padilla	Secretary	DHS	Represented by Jitendra Chandna
Robert Green	Secretary	DPSCS	Represented by Stanley Lofton
Dennis Schrader	Secretary	MDH	Represented by Matthew Otwell
Timothy Gowen	Adjutant General	DMIL	Represented by Brig. Gen. Adam Flasch
Russell Strickland	Director	MEMA	Present
Woodrow Jones	Superintendent	MSP	Represented by Maj. Tawn Gregory
Gregory Slater	Secretary	MDOT	Represented by Ken Hlavacek

Proposed Motion: Vote to Approve Meeting Minutes from August 3, 2020 (Chip Stewart)

Moved - Eric Lomboy
Second - Stanley Lofton

Stewart: Is there any debate or discussion?

Stewart: Are there any who are opposed to approving the meeting minutes from August 3, 2020? If so, please say "Nay."

Nay-0

Jitendra Chanda mentioned that he was not present for the previous meeting, following the approval.

Subcommittee Formation (Laura Gomez-Martin)

The Department of Information Technology (DoIT) will be forming subcommittees over the coming months that will develop processes, supporting documents, and guidance on various topics. DoIT is accepting requests from council members to participate in the subcommittee(s).

Laura Gomez-Martin recently joined DoIT as the new Deputy State Chief Information Security Officer. Her background focuses on policy and technology law, specifically where these two fields intersect. In her previous roles, she considered how the two areas influence each other and contribute to the security posture of organization. At DoIT, she will continue this work leading Governance, Risk, and Compliance.

Gomez-Martin presented on the goals and objectives of the subcommittees.

Council subcommittees (2):

1. **Authority to Operate (ATO) and Systems Security Plan (SSP)** - a document that is awarded through the ATO process and begins with a systems security plan (SSP). The requestor fills out the SSP, which seeks information such as, but not limited to: what the product is, its purpose, who the product owners are, and the security controls and parameters that will be in place before the product goes live. The Office of Security Management (OSM), at DoIT, will receive these requests.
2. **Request For Proposals (RFP)** - the objectives are to identify appropriate security requirements for RFPs, to avoid having irrelevant requirements, and to issue guidance for wording in agency templates, etc.

If there is interest in joining one of these subcommittees, please contact Chip Stewart (Chip.Stewart@maryland.gov) or Laura Gomez-Martin (Laura.Gomez-Martin@maryland.gov).

Jitendra Chanda, DHS, stated that MDTHINK currently uses the ATO process, and that agencies may need to abide by federal government requirements. In those situations, Mr. Chanda inquired as to whether Maryland agencies will have to follow both state and federal requirements.

Chip Stewart responded that this will need to be considered during the subcommittee.

DoIT Policy Catalog, Stewart

Over the past months, DoIT has revamped and consolidated much of the IT Policy Catalog (https://doit.maryland.gov/policies). Some of these relate to how units work with DoIT, others are more operational, but many of these are cybersecurity related.

Electronic Recording- This should be relatively non-controversial. With the shift to telework, there is a massive shift to online collaboration. There are also add-ons and services record and transcribe. They frequently store the data in the cloud, and could contain PII or PHI. They may not notify participants about recording. This policy is aligned with Maryland law.

Vulnerability Risk Management - Based on the data from the past year, this is the biggest reduction of risk.

Boundary Protection Baselines - Second most impactful initiative when looking at the events of the past year. This requirement is consistent with CIS top 20.

Supply Chain Risk Management (SCRM), Gomez-Martin

The threat to supply chains is growing, as cybercriminals are making use of vulnerabilities in these supply chains.

Solarwinds is one example of a supply chain risk. Solarwinds has three, potentially four, publically discovered vulnerabilities but this number continues to increase and impact organizations worldwide.

In Supply Chain Risk Management we must strengthen risk management practices and address Shadow IT by:

- Considering the purpose of a tool, determine what information needs to be collected (to avoid collecting more information than is necessary), consider how we collect the necessary information.
- Streamlining risk management processes to encourage users to use the proper channels. We do not want to discourage users from using the proper channels.
- Streamlining the analysis process so that it is repeatable.

Chanda, DHS, inquired whether this will be a part of the procurement process. Stewart responded that Chanda's assistance will be valuable in the subcommittees, since he has a lot of context.

Major Incident Overview

What we have seen in the last year….

- Exploit of public facing applications, eternals remote service (combinations of the first two, along with valid accounts has been a very successful combination);
- Phishing (has been low, so investment in security training shows valuable),
- Supply chain compromise

Major Gregory requested the slides from today's meeting.

Chip Stewart responds that a PDF of the slides will be distributed to all meeting panelists.

New Business

Director Landon, GoHS, asks for a status on NCR Grant money. Stewart responded that DoIT is tracking it. Director Landon would like Blake Langford (MEMA) included in the tracking.

Adjournment

Stewart suggested that a member make a motion to adjourn the meeting.

Proposed Motion: Vote to adjourn January 28, 2021 Maryland Cybersecurity Coordinating Council Meeting.

Moved-Stanley Lofton, DPSCS
Second- Director Landon, GoHS

All those not in favor of adjourning the Maryland Cybersecurity Coordinating Council please say "Nay."

Nay-0

Meeting adjourned: 9:37am

The next quarterly meeting is to be scheduled for April 2021.

Chairman of Board APPROVAL Charles I Stewart IV (Apr 21, 2021 09:30 EDT) Date: Apr 21, 2021