Maryland Cybersecurity Coordinating Council

Meeting Minutes

July 17, 2024 at 10:30 a.m.

Welcome (Greg Rogers)

The opening remarks included an expression of gratitude for everyone's attendance, an explanation that the previous meeting was canceled due to the Francis Scott Key Bridge collapse, and an overview of the agenda.

Roll Call/Call to Order (Greg Rogers)

Member Unit	Member Title	Voting Status	Member	Attendance
State CISO	State CISO	Chair	Greg Rogers	Greg Rogers
Aging	Secretary	Voting	Carmel Roques	Jonathan Jenkins
Agriculture	Secretary	Voting	Kevin Atticks	Carrie Deboy
Budget & Management	Secretary	Voting	Helene Grady	Derek Rost
Commerce	Secretary	Voting	Kevin Anderson	Kim Mentzell
Disabilities	Secretary	Voting	Carol Beatty	Not present
Emergency Management	Secretary	Voting	Russ Strickland	Secretary Strickland
Environment	Secretary	Voting	Serena McILwain	James Purvis
General Services	Secretary	Voting	Atif Chaudhry	Not present
Health	Secretary	Voting	Laura Herrera	Matt Otwell
Housing & Community Development	Secretary	Voting	Jake Day	Not present
Human Services	Secretary	Voting	Rafael López	Dennis Webb
Information Technology	Secretary	Voting	Katie Savage	Greg Rogers
Juvenile Services	Secretary	Voting	Vincent Schiraldi	Michael Pryor
Labor	Secretary	Voting	Portia Wu	Not present
Natural Resources	Secretary	Voting	Josh Kurtz	Miti Patel
Planning	Secretary	Voting	Rebecca Flora	Ted Cozmo
Public Safety & Correctional Services	Secretary	Voting	Carolyn Scruggs	Stanley Lofton
State Police	Superintendent	Voting	Lt. Col. Roland Butler	Major Tawn Gregory
Transportation	Secretary	Voting	Paul Wiedefeld	Shafiq Rahman
Veterans Affairs	Secretary	Voting	Anthony "Tony" Woods	Not present
Maryland National Guard	Adjutant General	Voting	Janeen Birckhead	Brig Gen Amy Kremer
Governor's Office of Homeland Security	Executive Director	Voting	Adam Flasch	Travis Nelson

Department of Legislative Services	Executive Director	Voting	Victoria Gruber	Not present
Administrative Office of the Courts	CIO	Voting	Bob Bruchalski	David DelGaudio
University System of Maryland	Chancellor	Voting	Jay Perman	Michael Eismeier & Mark Cather
Senate of Maryland	Representative	Non-Voting	Bill Ferguson	Not present
Maryland House of Delegates	Representative	Non-Voting	Nicholaus Kipke	Not present
Judiciary	Representative	Non-Voting	Judge Fred Hecker	Dave DelGaudio
State Chief Privacy Officer	SCPO	Voting	Caterina Pangilinan	Cat Pangilinan
State Chief Data Officer	SCDO	Voting	Open	Not present

Call to Order and Administrative

The November 14, 2023 meeting minutes were approved following a motion to approve by Secretary Strickland which was seconded by Derek Rost.

Mr. Rogers discussed the process for approving a delegate to the MCCC. He emphasized the importance of focusing the MCCC on cyber leadership. However, he clarified that if an agency does not have a dedicated person in that role, it is acceptable for the Secretary to advise Mr. Rogers to appoint someone in cyber as a delegate to ensure the highest quality advice is received from the agencies.

Organizational Changes/Cybersecurity Points of Contact

Mr. Rogers discussed the key points of contact within OSM:

- **Lance Cleghorn, Director of State Cybersecurity**: For services-related inquiries, particularly through the ISO program, agencies should reach out to Lance.
- **Mike Lavine, Director of Governance, Risk & Compliance**: For policy-related matters.. He will be developing an extensive library of security standards and guidelines to assist in implementing policies across systems. Please contact him with any policy-related questions.
- **Chris Krawiec, Director of Cyber Resilience**: For incidents and SOC-related matters, including testing and vulnerability management. Every agency is required to report incidents to OSM. You can do this via the incident reporting form on the DoIT website, by emailing the SOC, or calling the DoIT Service Desk (selecting option 5 will connect you directly). While multiple reporting options are available, using the phone number is preferred.

Legislative and Policy

Mr. Rogers addressed SB812 remediation, noting that agencies should have received an email last year requesting a remediation plan based on their cybersecurity assessment. Lance's team will be reaching out to discuss the necessary actions to meet these requirements.

He also discussed the System/Application Inventory initiative, noting that phase 1 for critical systems is now underway. Mr. Rogers stated that the Secretary is seeking a comprehensive list of critical systems to inform planning for MITDPs and statewide modernization efforts. There are legislative mandates to meet: by December, OSM must gather this inventory from all agencies, and by December, the State CDO will compile the data inventory. The goal is to streamline the process by consolidating these two inventories into a single, unified inventory.

Mr. Lavine addressed several key policy areas he is working on:

- Banned Hardware and Software, Authorization to Operate (ATO) Systems, and efforts being made to streamline governance processes leading to SOC reports to service providers.

- Offshore Software Development: A formal policy document will be issued to outline restrictions on off-shore development. The objective of which is to prevent the use of protected data classes in offshore development.

Additionally, Mr. Lavine expressed interest in establishing a peer review group and mentioned that governance will be a key aspect of the policy framework.

Mr. Rogers noted that the GRC team in OSM are working to create a Governance, Risk, and Compliance (GRC) framework that will cover the entire Executive Branch, eliminating the need for individual agencies to develop their own security controls and standards. The goal of this centralization is to implement a unified tool across all agencies.

DoIT Services: Cybersecurity Service Updates

Mr. Krawiec discussed the Bug Bounty Program, an initiative to test both public and private assets. This program provides access to trusted, vetted researchers who can identify vulnerabilities, enhancing overall security. The Bug Bounty Program expands the scope of vulnerability identification, with a particular focus on assessing the State's internet exposure.

Mr. Krawiec also went into other areas within his portfolio which includes Vulnerability Management falling under the Attack Surface Management team, with improvements focusing on the type of information shared. The MD-ISAC/Threat Bulletins area with the aim is to ensure that agencies are aware of advisories and understand what the response was and to take proactive measures in response to emerging threats. The Maryland Security Operations Center (MD-SOC) with an emphasis placed on clear communication, ensuring that when issues are reported, agencies understand the problem, the response, and where responsibilities lie. Ns finally Adversary Emulation with the focus on understanding how state agencies have leveraged their technical services to enhance their defenses.

New Items

Mr. Cleghorn discussed the centralization of the ISO program and some key upcoming centralized solutions:

- **Enterprise Attack Surface Management:** This tool utilizes credentials to aggregate read-only services across the enterprise, providing a comprehensive view of the attack surface.
- **Email Security**: This solution addresses phishing by using AI to analyze email content at an atomic level. If the data is deemed safe, it remains untouched; however, if it appears unsafe, it is documented along with the reason for the flag. Email Security adds an extra layer of protection against phishing attacks.
- **Password Management Solution**: A password management solution that will be available statewide. An onboarding kit will be provided to help users get started with 1Password. Initially, the focus will be on informing your user community about this tool.
- **Bug Bounty Program**: Targets public-facing assets to identify potential vulnerabilities, offering effective ways to mitigate risks.

Mr. Rogers acknowledged that the meeting did not cover the typical services provided by OSM. He advised that, if you have any questions about these services, to please reach out to your POs or any of the contacts listed in the POC list.

Open Discussion/Questions

Mr. Rogers opened the floor for questions and comments.

Derek Rost asked whether Email Security would replace DLP or be an additional layer. Mr. Rogers clarified that it would not replace DLP.
Matthew Otwell inquired whether the State IT Security Manual would be updated or replaced as part of the policy improvement process. Mr. Rogers responded that policy statements will be reassessed to determine their current relevance, and additional controls will be introduced as needed.
Derek Rost also asked whether there is a schedule around the bi-annual cybersecurity audit, noting that we are just about due. Mr. Rogers replied that the RFP is currently under review, and the immediate goal is to remediate findings before conducting the next assessment.
Carrie Deboy raised concern regarding SaaS platforms like Salesforce, asking how the state is addressing the use of add-ins and various software components, and whether an "approved" or "vetted" list of modules is being developed as the state needs to get in front of this. Mr. Rogers confirmed that Mike's team is working on creating an approved product and vendor list, aiming to align with lists from NSA or the State Department to ensure compliance with government standards.
Derek Rost added that many vendors are now incorporating AI into their products. Mr. Rogers acknowledged this and mentioned that AI is being integrated into the state's natural processes.
Derek Rost further inquired whether 2FA for Windows/AD is on the horizon. Mr. Rogers confirmed that it is and 2FA is a critical control for preventing cyber takeovers.
Dennis Webb asked if there are plans to add phishing simulation testing to validate the Security-IQ training. Mr. Rogers noted that this is a topic of frequent discussion but mentioned that the industry is shifting away from phishing testing. Many CISOs believe phishing testing has limited impact on adversary security, especially with more efficient tools like Abnormal.
LTC (MD) Laurie Kwiedorowicz from the Maryland Defense Force acknowledged their attendance at the meeting.

Next Meeting Date

October 2024 (Date to be determined)

Adjourn

Motion to adjourn by Greg Rogers, second by Major Tawn Gregory.