Maryland Cybersecurity Coordinating Council

Meeting Minutes

May 21, 2025 at 11:00 a.m.

Welcome (James Saunders)

The meeting began with a welcome and appreciation for attendees joining the MCCC meeting.

Roll Call/Call to Order (James Saunders)

Member Unit	Member Title	Voting Status	Member	Attendance
State CISO	State CISO	Chair	James Saunders	James Saunders
Aging	Secretary	Voting	Carmel Roques	Jonathan Jenkins
Agriculture	Secretary	Voting	Kevin Atticks	Not Present
Budget & Management	Secretary	Voting	Helene Grady	Derek Rost
Commerce	Secretary	Voting	Harry Coker, Jr.	John Papabasiliou
Disabilities	Secretary	Voting	Carol Beatty	Elizabeth Hall
Emergency Management	Secretary	Voting	Russ Strickland	Meredith Lang
Environment	Secretary	Voting	Serena McILwain	Gary Anastasio
General Services	Secretary	Voting	Atif Chaudhry	Not Present
Health	Secretary	Voting	Meena Seshamani	Matt Otwell
Housing & Community Development	Secretary	Voting	Jake Day	Not present
Human Services	Secretary	Voting	Rafael López	Dennis Webb & David Heller & Dave Sloan
Information Technology	Secretary	Voting	Katie Savage	Jason Silva
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 & Amaro Thames
State Police	Superintendent	Voting	Lt. Col. Roland Butler	Major Tawn Gregory
Transportation	Secretary	Voting	Paul Wiedefeld	Not present
Veterans Affairs	Secretary	Voting	Ross Cohen	Not present
Maryland National Guard	Adjutant General	Voting	Janeen Birckhead	Craig Hunter & Patrick Hawkins
Governor's Office of Homeland Security	Executive Director	Voting	Adam Flasch	Travis Nelson
Department of Legislative	Executive Director	Voting	Victoria Gruber	Not Present

Services				
Administrative Office of the Courts	CIO	Voting	Bob Bruchalski	Robert Bruchalski
University System of Maryland	Chancellor	Voting	Jay Perman	Michael Eismeier
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	David DelGaudio
State Chief Privacy Officer	SCPO	Voting	Caterina Pangilinan	Not Present
State Chief Data Officer	SCDO	Voting	Natalie Harris	Not Present

Additional Attendees	**Title**
Howard Barr	DoIT AAG
Patrick Mulford	DoIT Chief of Staff
Chris Krawiec	DoIT OSM Sr. Dir of Cyber Resilience
Lance Cleghorn	DoIT OSM Sr. Dir of State Cybersecurity
Travis Edwards	DoIT OSM Sr. Dir of Local Cybersecurity
Miheer Khona	DoIT OSM Dir. of GRC

Call to Order and Administrative

The February 19, 2025 meeting minutes were approved by Stanley Lofton and seconded by Jason Silva.

OSM Updates

Mr. Saunders provided an overview of the Office of Security Management (OSM) organizational chart, from the Department of Information Technology (DoIT) Secretary to the OSM Directors.

State Cybersecurity

Mr. Cleghorn introduced his team and discussed the State's cybersecurity. The team members are:

- Johnny Miranda: Director of Cyber Engineering
- Ian Roberts: Director of ISO Program
- Carl Arce: Deputy Director of Cyber Engineering

He further discussed improving alignment by the team working to centralize all cybersecurity platforms back into OSM. The focus will be on developing clear product roadmaps, comprehensive documentation, and providing adoption assistance to agencies. A key goal is to bring on a Director and Service Delivery Manager. These efforts align with OSM's overall service offerings:

- ASM (Attack Surface Management)
- SOC (Security Operations Center)
- CTI (Cyber Threat Intelligence)
- ISO (Information Security Officer)

Mr. Roberts presented the ISO program and its seven-phase roadmap to cybersecurity maturity:

- Phase 1: Onboarding and Stakeholder Identification

- Phase 2: Initial Assessment - Develop a weakness evaluation report to identify gaps
- Phase 3: Remediation
- Phase 4: Posture Assessment - Conduct a supplemental cybersecurity maturity evaluation to introduce a roadmap to agencies
- Phase 5: Control Enhancement - Identify necessary cybersecurity controls
- Phase 6: Service Documentation and Policy Standardization
- Phase 7: Governance – Guidance on governance and risk-based assessment

He expressed his desire for the ISOs to be the face of agencies. He also requested feedback on what is working well and what could be improved within the new ISO program. There was discussion on key projects and initiatives particularly 1Password - invitations were sent to all DoIT-managed agencies and currently working with ISOs to extend invitations to non-DoIT agencies, Cloudflare - Engineering Director working on Cloudflare is focused on the executive branch; approximately 70 DNS zones have been migrated with work being done to migrate the remaining 100+; an effort is underway to build Cloud Security Posture Management into centralized service across agencies, and Abnormal is currently enabled for all @maryland.gov and @msd.edu addresses; the team is actively beta testing the Graymail function to manage vendor spam email.

Governance, Risk & Compliance

Mr. Khona addressed the rationale for updating the IT Security Manual from a GRC perspective. The current policy structure suffers from inconsistencies, has role-centric attachment - applicable policies are duplicative depending on role functionality, and need to respond to change. The goal is to address these issues by:

- Streamlining and Aligning - ensuring a consistent application of security policies across the state
- Separating Guidance from Implementation - decoupling directional guidance ("what") from the specific steps for implementation ("how")

He noted that the Next-Gen Maryland Cybersecurity Policy Framework codifies different elements of a policy suite. The basis for the Cybersecurity policy structure is zero trust - shifting away from a traditional trust model to a "never trust, always verify" approach, clear direction - providing unambiguous guidance to all users, statewide alignment - directly aligning with the state's risk profile, and a user-centric design - making it easier for different user groups to absorb necessary information and manage their cyber risks effectively. The structure is organized to ensure statewide consistency:

- Tier 1: State Cybersecurity Governance Policy
- Tier 2: Functional Policies
- Tier 3: Cybersecurity Standards

This layered approach ensures clear governance while providing flexibility for agencies to implement standards and procedures tailored to their unique environments. The entire policy suite is tied to the NIST CSF. The timeline for this rollout is development: November 2024 – May 2025, feedback & adjudication: June – September 2025, and tentative launch: October 2025.

Local Cybersecurity

Mr. Edwards provided an update on the ongoing assessments. To date, 11 assessments are in progress, with another 18 in the queue. Since January 2025, the team has dedicated approximately 620 hours to assessment and risk management support. The assessment process is providing valuable insights into cybersecurity at the local level. Findings indicate that 85% of scores for subcategories are 0s and 1s, pointing to inconsistent or non-performance of security programs. The low scores can primarily be attributed to four key factors 1) limited staff - little to no dedicated cybersecurity personnel, 2)

insufficient budget - small or shrinking budgets for cybersecurity, 3) lack of awareness - jurisdictions are unaware of core cybersecurity domains, controls, or functions, and 4) resource constraints - insufficient resources to mature their security programs. To help address these gaps, the team is implementing several key support measures after each assessment:

- Risk Prioritization - helping jurisdictions understand their most critical risks
- Knowledge Gap Education - providing education to fill knowledge gaps identified in the assessments
- Documentation Assistance - assisting with putting templates in place to govern, a significant gap at the local level
- Best Practice Integration - helping agencies incorporate best practices into their processes
- Low/No-Cost Resources - identifying and leveraging low or no-cost resources to fill program gaps
- Funding Pathways - providing pathways to funding when resources are exhausted, including:
    - SLCGP Year 3: A federally funded grant program, $4.9M/30% cost share
    - Local Cyber Support Fund: A new, non-lapsing $3.5M fund from Maryland with specific eligibility requirements; currently working with MDEM on the application process

State Cyber Resilience

Mr. Krawiec provided an overview of the core programs within the Cyber Resilience function:

- Security Operations Center (SOC): Continuous security monitoring and threat tracking
- Cyber Threat Program: Identifying and analyzing threats and threat intelligence
- Attack Surface Management (ASM): Vulnerability identification and remediation
- Adversary Emulation Program: Integrates insights from the core programs to create actionable assessments; key objective is to better operationalize threat intelligence by taking identified threats and incorporating them into the threat hunt program

His team is currently working on two significant initiatives, 1) Vulnerability Disclosure Program, and 2) Hack the State 2.0 that is scheduled to be executed this summer. Also rolling out Service Summit to gather feedback and provide updates on services, enhanced program & service documentation via the ISOs, and in the process of cyber insurance policy.

Open Discussion/Questions

Mr. Saunders opened the floor for questions and comments and inquired about feedback to make the MCCC more meaningful.

Next Meeting Date

August 13, 2025

Adjourn

Motion to adjourn by Stanley Lofton, second by Jonathan Jenkins.