Maryland Cybersecurity Coordinating Council
Meeting Minutes
August 20, 2025 at 10:30 a.m.

Welcome (James Saunders)

Mr. Saunders welcomed the attendees to the MCCC meeting and noted a full agenda today. He provided an overview of the agenda topics and stated that questions can be brought up at any time for interactions within the topics.

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	Not Present
Commerce	Secretary	Voting	Harry Coker, Jr.	Not Present
Disabilities	Secretary	Voting	Carol Beatty	Not Present
Emergency Management	Secretary	Voting	Russ Strickland	Not Present
Environment	Secretary	Voting	Serena McILwain	Not Present
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
Information Technology	Secretary	Voting	Katie Savage	Jason Silva
Juvenile Services	Secretary	Voting	Vincent Schiraldi	Michael Pryor
Labor	Secretary	Voting	Portia Wu	Tae Rim & Tara Murphy
Natural Resources	Secretary	Voting	Josh Kurtz	Not Present
Planning	Secretary	Voting	Rebecca Flora	Doug Lyford
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	Jay Bommus
Veterans Affairs	Secretary	Voting	Ross Cohen	Not present
Maryland National Guard	Adjutant General	Voting	Janeen Birckhead	Craig Hunter

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	Robert Bruchalski
University System of Maryland	Chancellor	Voting	Jay Perman	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	David DelGaudio
State Chief Privacy Officer	SCPO	Voting	Caterina Pangilinan	Caterina Pangilinan
State Chief Data Officer	SCDO	Voting	Natalie Harris	Natalie Harris

Additional Attendees	**Title**
Chris Krawiec	DoIT OSM Sr. Dir of Cyber Resilience
Lance Cleghorn	DoIT OSM Sr. Dir of State Cybersecurity
Steven Burke	DoIT OSM Acting Dir of Local Cybersecurity
Miheer Khona	DoIT OSM Dir. of GRC

Administrative

The May 21, 2025 meeting minutes were approved by Jason Silva and second by Natalie Evans Harris

Org Structure

Mr. Saunders provided updates to the organizational structure within the Office of Security Management (OSM)and noted that privacy is now back to being part of OSM. He added that they are excited to drive partnership with privacy across the state. Mr. Saunders also noted that Travis Edwards has departed the state as the Director of Local Cybersecurity and Mr. Steven Burke is the acting local cyber director to continue to foster the local cyber space.

IT Master Plan Cybersecurity:

Mr. Saunders announced that last week DoIT released the IT Master Plan and discussed the highlights of the master plan as it relates to cyber and the five goals. He welcomed any further deep dives in future discussions. He stated that the partnership goal is key for these meetings and getting toward critical infrastructure as well.

Mr. Saunders broke out the key goals and went into a high-level discussion as it relates to the approach of goal:

A. Planning for resilience and high availability.

B. Work on the cyber policy and framework with “GRC as a service,” currently in its initiation phase.

C. Develop services that agencies want to use that are valuable, cost effective, and have good working relationships with OSM which will build roadmaps and mechanisms over time.

D. Promote statewide collaboration via this forum, working groups, and other avenues while ensuring statewide contracts clauses are put in place.

E. Work with Labor with the COMET program and Commerce to leverage businesses across state to develop services and training to meet these goals.

Toolshell Incident Overview

Mr. Krawiec began by discussing what has been worked on over the last month as it relates to the toolshell incident. He provided a background as to when the first recognition of something was going on and when Microsoft acknowledged there was exploitation occurring. He noted discussion on the CVE's and how they were part of the toolshell event and Sharepoint version impacts (2013, 16, 19 and subscription edition). He stated that the drive of patching and adoption of mitigating controls as critical parts of the effort to resolve including a statewide impact assessment, who was using the versions, the vulnerabilities, patching, and observations of activity of compromise.

Mr. Krawiec went on to discuss impacted servers and notable deployments and the work performed to continue to secure the state and prevention of exploitation. He advised that end of life (EOL) instances need to be modernized to better prevent future risk to the state. He also noted that MD-ISAC is a good avenue for dissemination of important events and is a path to get in touch with key IT leaders that need to know what is happening. He stated that OSM did send out data call for feedback to state cyber leads-re cyber toolshell for feedback by end of the week and to check inboxes (sent yesterday 2pm) as there is a survey link there to take a few minutes to share feedback and engagement and learning opportunities.

BODs

Mr. Saunders brought forward that there are three operational directives currently in flight:

1. Mandatory enrollment to MD-ISAC- Enrollment is at 90 % of all state agencies, 95% locals, but municipalities are less than 10%. He noted that what would also be included is all state contractors as some agencies outsource to a third-party supplier. Mr. Saunders stated that if you are part of the state, doing business with the state, you must be enrolled in MD ISAC and that it is no cost to join the MD ISAC.
2. Public Website Security - Mr. Saunders noted that if this BOD was in place, it would prevent some of the effects of the toolshell type incidents. He noted extending the service of Cloudflare (WAF) to all of Maryland's websites, at no cost to agencies, and has learned there are a variety of domains across the state which he will work with the DoIT digital services team to consolidate top level domains, particularly. gov. He stated that it is critical to standardize and understand what EOL software is in place, the need to develop migration plans for EOL SW, and ensure a plan is in place including budgets to support this modernization.
3. VDP- Mr. Saunders stated that as this is an industry standard, we should bring Maryland into the fold by obtaining good security researchers to provide information about our services, and ensure appropriate guidelines are in place for doing so.

Question -
Mr. Otwell asked about the public website security BOD and if this is an executive directive for all agencies to convert to .gov for all websites? He stated that he was very supportive of this BOD and what the expectation on the timeframe to release was?

Mr. Saunders stated that as written currently, yes, needs to standardize in TLDs and as for timeline, its going through adjudication process-which ends this Friday with final anticipation of release is mid-late September.

Mr. Nelson highlighted that the MD ISAC enrollment piece is critical for those in the exec branch and the governor's office is highly recommending this enrollment before it's mandated.

Mr. Rim posed two questions for Mr. Krawiec which asked which tools, like bug crowd, is OSM looking to promote and will it eliminate duplication of findings and also if there are thoughts to expand Nessus scanning.

Mr. Krawiec responded that bug crowd is sourced to support triage and validation prior to release to agencies with applicable minimum standards and that they are working to expand the scope of other services like Nessus web scanning.

MCCC Working Group

Mr. Saunders noted that this meeting can never be the only forum for engagement and interactions and built working groups to enhance collaboration and discussion regarding the cybersecurity strategy, to bolster cyber knowledge, and introduce shared ownership. He stated that the first working group was formally announced June 16, 2025 and that two more will launch in October.

Customer Advisory Board

Mr. Krawiec spoke of collaboration, the relationship to the ITMP, and the goal to deliver stronger services. He stated this board/working group will be an open discussion of OSM services performance, its challenges and improvements, and the desire to run the services from the consulting perspective. Mr. Krawiec stated that OSM wants to understand how they can support agencies and needs, where agencies are struggling, and where help is needed. Mr. Krawiec is working on the charter, schedules, and other deliverables. He noted that Ian Roberts will co-chair the working group and the ISO program will work in tangent on this board and that the team is working to formalize a method of receiving feedback and ensuring there is a documented process and the opportunity for service summits and the services being delivered. He stated that they plan to be ready for the first meeting by October 22nd.

Zero Trust

Mr. Cleghorn spoke on Zero trust with Steven Burke co-chairing and that OSM is steering towards meeting the master plan objectives with this work group. He stated the need to bring folks across the state to discuss mission focused topics, and zero trust, which is not immediate but is a journey with milestones that need to be outlined. Mr. Cleghorn wants to ensure local partners are included in this and with NetworkMD supporting the whole of state approach to manage cyber security. He stated that around September 17th that the charter, schedule and what deliverables to deliver back to MCCC can be shared with a kickoff to be held October 15th. He stated that if interested in joining, feel free to reach out to ISO.

Governance, Risk, and Compliance

Briefing on Policy Suite Transition

Mr. Khona introduced the GRC working group and the milestones they have; discussed the current state across four areas- IT Security policy (high level); Tier 3 IT Security. Manual and technical policies standards; Tier 2 directives (BOD and Emergency) to address immediate threats, and Tier 1 being the catch all policies developed. He stated that the current challenge is navigation difficulties, unclear responsibilities and inconsistent guidance. Mr. Khona then went on to the future state and was grateful for incredible expertise and experience on comments for batch 1 with batch 2 in process for comment. Mr. Khona discussed the hierarchy and the replacement of polices, what other functional policies will exist, and the rules to explain the why, which replaces parts of the security manual. He stated that tier 3 replaces technical components in manual and are directly aligned to NIST control families and this new model will be easier to navigate, easier to find, easier to update, less confusion as it organizes by topic not user role, and reduces duplication and ambiguity.

Mr. Saunders added that while we are working on a new security and policy suite there is the need to start change management mapping of what we used to do, to what we do in the future, how we convey this conversation and the minimum standards to convey the changes to all groups. He noted being open to feedback on approach and

steps towards this transition.

Mr. Khona went on to discuss the broader risk management program and the roll out of the policy suite, where to start with a maturity model and the level to implement critical controls and to move to 100% compliance. He went on to discuss end to end timeline as the team is currently in batch 2 cycle with 58 reviewers from respective agencies in addition to some local govt partners/counties. He looks to wrap up at the end of October with full review cycles complete and then in November and December to finalize elements with broader life cycle management, building the communication plan, and developing linkages between documents for navigation of the topics.

Foreign Travel Review

Mr. Krawiec discussed what observations were occurring from foreign travel and major evolution started August 5th, implementing alerting into MD SOC, and taking log sources for OCONUS instances and movement between locations. He stated from there the MD SOC obtains tickets, investigates foreign travel if it matches in the authorized foreign travel list, and takes next appropriate action/steps to ensure protection of assets and state data.

Mr. Saunders added as to the key devices that there is no bring your own device (BYOD) policy at large but would like to obtain stance on Maryland's BYOD thoughts from agencies and the business/mission focus and how policies should be addressed; open to participants sending emails and thoughts to Mr. Saunders.

ISO Updates

Mr. Roberts discussed the key milestones of the ISO program and projected a good story of the program with closing security gaps and building strong partnerships and updating remediation statistics. He noted that there will be a cyber posture questionnaire for the next assessment cycle. Mr. Roberts stated that the next steps in preparation for next assessment cycles will include completion of CAP remediations, closing the POAMs, and partnering with GRC for standard policies and templates. Mr. Roberts touched on BCR training to cyber professionals to improve collaboration and education to support the program.

Mr. Cleghorn added that they are approaching the end of the eighth month of the program, looking at what went well, could have gone better, and how to best service agencies with already strong cybersecurity talent and level of support and end of year report.

MS-ISAC/MD-ISAC Update

Mr. Saunders touched on his thoughts on ISAC, with funding cuts on CIS and ISAC. Mr. Saunders is looking at the options for the whole of state, inclusive of agencies, local, K2, etc. but the cost is not currently included in the budget. Mr. Saunders continued conversations with other state CISOs and agencies interested in joining. Mr. Saunders stated that he will continue to work with MS- ISAC and work on a cost- benefit analysis to determine the best course of action is needed.

Mr. Krawiec touched on the MD- ISAC and its offerings and ensured better leveraging of the tools within the cyber threat program. MS- ISAC does have other additional service offerings that MD ISAC is looking into. He noted that the team is working to start more recurring threat briefings that may be of interest to the state and inclusion of listening sessions.

Open Discussion

No topics were brought forth for open discussion.

Next Meeting Date

Next anticipated: Wednesday November 5, 2005 (2:30pm-4:00pm)

Adjourn
Motion: Travis Nelson
Second: Jason Silva