Date: August 8, 2019
Time: 10:00am - 11:30am
Location: 100 Community Place, Crownsville, Maryland 21032

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Maryland Cybersecurity Coordinating Council Meeting
Meeting Minutes

Council Members in Attendance

- John Evans, State Chief Information Security Officer
- Linda Singh, Adjutant General, Military Department (MIL)
- David Brinkley, Secretary, Department of Budget & Management (DBM)
- Ellington Churchill, Secretary, Department of General Services (DGS)
- Robert Green, Secretary, 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)

Call to Order: John Evans, 10:04 a.m.

State of Maryland Cybersecurity Challenges

John Evans: Advised that there are 67-86 state agency directorates. There are many cyber practices taking place across these agencies--some of which are inconsistent. There is a lack of visibility and consistent tools which result in additional--and unnecessary--costs for the state. The Maryland Department of Health was the first agency to use the DoIT's Enterprise tool—this one tool alone saved the department $24,000. Millions of dollars can be saved through consolidating various tools moving forward.

Executive Order

John Evans: Stated that Governor Hogan is very committed to cybersecurity. Under Governor Hogan, Maryland established its first state CISO and created the first Maryland Cybersecurity Coordinating

Council (MCCC). Two primary objectives and roles of the CISO are assessments and consolidation. It is important that all branches operate consistently to keep our agencies--and all information within the agencies--safer. Procurements are being initiated on a statewide basis. Any security product being procured for an agency needs to be approved by John Evans before process can continue.

Superintendent Pallozzi: Asked for a definition of security.

John Evans: Clarified that any procurement relating to cybersecurity needs to be forwarded to him for his review and approval.

Information Technology Security Manual

John Evans: Stated that the Information Technology Security Manual has not been updated since 2013. His office recently published a new manual that offers more clarity and understanding. The manual is available on the DoIT website. In the near future, twelve (12) new policies will be added to the manual to provide more guidance.

Jitendra Chandna: Asked if we plan to build templates, policies, and procedures.

John Evans: Confirmed that this will be the case.

Risk Acceptance Memos (RAMS)

John Evans: Stated Risk Assessment Memos (RAMS) require buy in from everyone at the table. For example, if an agency has software/hardware that is out of compliance, the agency must submit a RAM to DoIT describing the out-of-compliance item. DoIT will conduct a risk assessment. Once done, the form will be given to the agency head and respective CIO for signature. Signatures signify that the agency head understands a risk exists for continued use of the out-of-compliance application and is willing to accept any consequences that may result.

Pete Landon: Wanted to know how something is deemed out of compliance.

John Evans: Currently we are relying on the honor system. DoIT purchased vulnerability scanners and found unencrypted personally identifiable information (PII).

Major General Linda Singh: Recommended that DoIT have a specification/checklist list. This is to ensure that requirements are being met. There should be no use of unsupported software (as an example).

Superintendent Pallozzi: Stated there is a difference between awareness and acceptance as a Secretary.

Major General Singh: Felt it is more complicated – that we need to prioritize and mitigate. For example, we are willing to accept because of the mitigating steps we are taking.

John Evans: Stated we follow the federal government's process. There is also a plan of action and milestones embedded in the assessment.

Major General Singh: Thought dual signatures should be on the form.

Secretary Brinkley: Thought it would be impractical to have a sign-off by every Secretary because each agency has a different size.

Major General Singh: Thought there are things we can put into place as an individual. We need to get people to do the right thing. She also thinks that MEMA needs to be specific to the vulnerability we are talking about.

Secretary Green: Agreed there should be multiple signatures.

Russell Strickland: Asked if agencies sign an agreement, will John Evans' office handle everything?

Mr. Evans: Confirmed that his office will handle. He expects DoIT staff to be onsite to handle situations even before a breach were to happen.

Secretary Green: Expressed a need for guidelines for future purchases around cloud storage and opportunities for that and guidance on what we should be looking at.

Secretary Churchill: Asked when DoIT is expected to complete the scanning of historical data for everyone to see.

Mr. Evans: Advised that DoIT currently manages thirty-five (35) agencies. DoIT's goal is to get this out sooner rather than later. Mr. Evans offered to pay for any agency who would like a vulnerability scanner.

Secretary Brinkley: Wanted to know who is tracking the contract and maintenance of the standard? At what point do you find they are out of compliance and how do you communicate?

Mr. Evans: Replied that what is supposed to be happening is we rely on a security or accounting firm that goes through the checklist to ensure processes are being followed by the vendor. This is stated in a standard RFP template. The vendor is supposed to give us a new template each year, as required in the contract.

Secretary Brinkley: Wanted to know whose responsibility it is to check the vendor.

Mr. Evans: Said the contract manager manages the documentation for their vendor. If this is custom code then DoIT would need to do an assessment. It could be a risk assessment if it is something small. If it is a full application, storing-data issue, then the process would be to create a system security plan.

Secretary Green: Standardization of language should be in all contracts. Should have expected practices.

Secretary Churchill: Expressed concern about procurement issues, but in the plan it is indicated that each agency has a CIO that works along with DoIT. Does each agency have to have a CIO?

Mr. Evans: Stated that DoIT will fulfill that obligation if an agency does not have an Information Technology team.

ACTION: Secretary Churchill would like to have an off-line discussion with Mr. Evans about this.

Agency Assessment Kickoff

Mr. Evans: Gave an overview about the positives of internal/external scores versus just internal or external separately. Mr. Evans stated that if anyone wants these installed to please let him know and his office can assist--if you want to show a more accurate view of what is happening in your environment.

MEMA Cyber Response Guidance

MEMA would be the coordinating agency around a cyber event. DoIT and OSM would lead the response.

National Guard Training – Starting with MEMA, to be rolled out to other agencies.

Homeland Security Program – Have a program coming up, working on correlation threat data worldwide. We are the first state in the nation to kick this off.

DOIT SECAAS

The Department of Information Technology is offering across the state: Security Operations Center (SOC) Vulnerability management Firewall management Security Awareness Training. DoIT has phishing campaigns that can be made available.

ACTION: If there are specific lines of training you want for your agency, please contact John Evans.

Recap:

Assessment Support

RAM Form Process

Questions and Answers:

Secretary Brinkley: Would like an opportunity to reach out to analysts and CIOs on assessment support.

Secretary Brinkley: Says pension system has a lot of money, the 529 board, 501k has money. At what point do our boundaries start and another picks up? Secretary Brinkley felt a conversation about this is needed. Secretary Brinkley recommended an intra-state council.

Secretary Neall: Recommended that we look at the Maryland Manual to see how many independent agencies are currently not being supported.

Major General Singh: Asked what is being done to secure our global cities--in this case, our state.

John Evans: Closed the meeting and stated he intends to have quarterly meetings. The meeting is to be scheduled for early to mid-November.

Mr. Evans: Asked that desired topics of discussion be submitted to him or to Maria Fisher.

Meeting Concluded at 11:33 a.m.

Chairman of Board APPROVAL Charles J Stewart III Date: 3/2/2020