Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

Office of Security Management

Cybersecurity 2023
Year in Review

Contents

2023 Year in Review 3
Message from the State Chief Information Security Officer 3
Legislative Updates 4
State Minimum Cybersecurity Standards 4
Statewide Cybersecurity Centralization Strategy 4
Incident Reporting for Utilities 5
Major Cyber Accomplishments of 2023 5
Cyber Resilience 5
Endpoint Managed Detection & Response (MDR) Service Status 5
Service Summits 6
MDCERT 6
Remote Access 6
Security Awareness Training 6
Agency Pilot Engagement on Security Templates 7
MD-ISAC Growth and Successes 7
Additional Service Accomplishments 8
MLCC Successes 8
State and Local Cybersecurity Grant Program (SLCGP) 10
MABE Cybersecurity Assessments for LEAs 10
Major Initiatives of 2023 10
Spotlight Capabilities added to MDR Service 11
Cybersecurity Asset Attack Surface Management (CAASM) 11
Centralized Logging Solution 11
Cybersecurity as a Team Sport 12
Statewide Cybersecurity Training Program 12
October Cybersecurity Awareness Month (OCSAM) 12

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

2023 Year in Review

Message from the State Chief Information Security Officer

As we close out another year, I am sharing our third Office of Security Management (OSM) Year in Review. While this is my first Year in Review, it is something that has been previously prepared by my predecessors. These prior reports have focused on the achievements of OSM, and this year is no different. I recognize not only what those before have accomplished, but we continue to build upon that critical foundation to improve both OSM's service and the State's overall security posture. Some of the key developments from those before me that we have continued to build upon are the Maryland Security Operations Center (SOC) and the MD Information Sharing and Analysis Center (ISAC). These two services are critical to effective detection and response to cyber events. Additionally, OSM has on-boarded more agencies to our endpoint detection and response, and vulnerability management services, as well as the managed firewall service. These services, and others, round out OSM's security centralization strategy to complete the full cybersecurity lifecycle from protection and detection to recovery and remediation. Overlaying all of this is the newly created Governance, Risk, and Compliance (GRC) function, which will provide the oversight and governance required to design and implement a modern, best practices-based state information security program.

Our focus and strategy going forward are to build upon the foundation that was laid by those in the State CISO role before me and deliver a centralized cybersecurity program to effectively and responsibly use our resources to reduce and consistently manage cyber risk to the State and its residents. DoIT's overarching goal with cybersecurity is to Leave No One Behind, therefore, we are taking an approach to a cybersecurity strategy that intersects State and Local governments and that reaches all Marylanders.

Gregory Rogers

Gregory Rogers
State Chief Information Security Officer

Legislative Updates

While 2023 did not see any new legislation of State cybersecurity, we continue to execute the requirements implemented by the previous year's bills. There were three key activities, outlined below, undertaken in 2023 to meet legislative requirements. They focused on the development of cybersecurity strategy, security standards, and incident reporting. Additionally, at the end of 2023 the State CISO joined the Cyber Maryland Board, created through HB 801, to help drive cyber workforce development within the State of Maryland.

State Minimum Cybersecurity Standards

Per Senate Bill 812 (2022), the Office of Security Management published on May 25, 2023, its State Minimum Cybersecurity Standards for the Executive Branch of State Government. The State of Maryland's Minimum Cybersecurity Standards align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), consisting of controls that contribute to an organization's overall cybersecurity maturity while mitigating or reducing cybersecurity risk and vulnerabilities.

Statewide Cybersecurity Centralization Strategy

The Statewide Cybersecurity Centralization Strategy was released in August 2023.
In accordance with Section 5 of SB812, Ch. 242 (2022), and in alignment with regulations established by DoIT, DoIT OSM diligently formulated this transition strategy towards cybersecurity centralization for Maryland's Executive Branch of State Government, henceforth referred to as the "State Cybersecurity Centralization Strategy."

The State Cybersecurity Centralization Strategy aims to achieve the following goals of Senate Bill 812:

1. Provide a strategy to "centralize the management and direction of cybersecurity strategy within the Executive Branch of the State Government under the control of the Department of Information Technology," and
2. "Serve as the basis for budget allocations for cybersecurity preparedness for the Executive Branch of State Government."

By implementing this comprehensive strategy and engaging in proactive collaboration, Maryland's Executive Branch will bolster its cybersecurity posture, ensuring the safety and security of critical assets and information for the benefit of all citizens and organizations within the State.

Incident Reporting for Utilities

In November 2023, pursuant to the requirements of Md. Code, State Public Utilities Article §5-306(D)(2), the State Chief Information Security Officer (SCISO), in consultation with the Public Service Commission, established criteria for a public service company to report cybersecurity incidents. These "Cybersecurity Incident Reporting Requirements for Public Utilities" Guidelines are posted on the Department of Information Technology (DoIT) cybersecurity webpage: Policies, Standards, and Guidelines.

Major Cyber Accomplishments of 2023

Over the course of the year OSM leadership and teams have been busy improving and rolling out new cybersecurity services. Below we have provided an overview of many of the incredible accomplishments of the dedicated teams and individuals within OSM, without whom we would be unable to develop and implement our security program. It is these activities that have improved collaboration across State and Local governments, built out new security offerings, and delivered enhancements to OSM services.

Cyber Resilience

DoIT's OSM established the Cyber Resilience portfolio in June 2023 and hired its first Director of Cyber Resilience. This portfolio demonstrates a commitment to centralize services and support in a whole-of-state approach to better deliver positive outcomes to agency and government partners with a multi-year approach to integrate OSM services into the Maryland Security Operations Center (MDSOC) and establish a fusion center capability.

Endpoint Managed Detection & Response (MDR) Service Status

In 2022, OSM introduced its Endpoint Managed Detection and Response (MDR) service. In 2023, this OSM service is now supporting more than 65 customers with visibility of more than 45,000 endpoint devices and monitoring more than 90,000 user accounts. The MDR service enables the formula of detection in seconds, response in minutes, and remediation in hours for all protected assets.

Service Summits

As the Year in Review for 2022 alluded to for 2023, OSM held three (3) key cybersecurity service summits; Endpoint Managed Detection and Response, Security Awareness Training, and the Maryland Information Sharing and Analysis Center (MD-ISAC). These summits brought together a number of key stakeholders and subject matter experts (SME's) both virtually and in person at DoIT allowing service overviews to be provided, questions to be asked, and concerns to be addressed. Cybersecurity Services by OSM continue to increase to units of government Statewide.

MDCERT

The MDCERT responded to six (6) major cyber incidents resulting in real time remediation of the incident in a truly cross-functional and interagency approach integrating elements of State Government, Local Government, Federal Government, and law enforcement partners. In accordance with Maryland policy the MDCERT recommended three of these incidents to be disclosed to the general public. This marked the first time that incidents were disclosed to the public in an effort to achieve a more transparent and open Government. https://doit.maryland.gov/cybersecurity/Pages/Public-Incident-Reports.aspx

Remote Access

Remote access is an important service provided by the Department of Information Technology Office of Security Management, to many units of State government, to permit employees, contractors, and vendors to access internal State resources remotely. With many agencies supporting work from home (WFH), remote access has become a critical service used to support the mission of many agencies. When strategizing about the future of this service and the renewal of the existing technology platform, DoIT OSM determined that migrating from a standalone virtual private network (VPN) solution to an existing platform already licensed for this service would improve efficiencies, cut costs, and consolidate technologies. This analysis and migration began in 2023 and is projected to be completed in 2024 with minimal interruption to customers.

Security Awareness Training

The primary objective of the security awareness training program is to strengthen the overall security culture throughout the State of Maryland by training employees how to recognize and respond to potential threats. In support of this objective, the Department of Information

Technology Office of Security Management (DoIT OSM) added role-based training as a new capability to its security awareness training service, in CY23.

Role-based training is a set of learning activities focused on providing employees with the knowledge and skills needed to securely perform their job. Eight (8) agencies enrolled in this new capability this year and DoIT OSM expects to see this number continue to grow as it is promoted to other agencies.

Cybersecurity is not only a critical component to strengthen the State of Maryland, but also key to bring cyber awareness to all citizens in Maryland. OSM is developing a public cyber awareness page on the DoIT Cybersecurity website that will provide useful cyber information, best practices, tips and will continue to house the Cybersecurity Awareness Month content.

Agency Pilot Engagement on Security Templates

OSM partnered with multiple agencies in the development of key security templates and accompanying procedures in the following cyber areas: risk management, incident response, and business continuity/disaster recovery. Three agencies participated in each of these cyber areas. At the conclusion of this pilot, these agencies were able to have fully developed plans in their specific pilot area. This not only educated the agencies in these cyber areas but also, provided a vehicle to support the remediation of key findings from their security assessments.

MD-ISAC Growth and Successes

The Maryland Information Sharing and Analysis Center (MD-ISAC) has experienced significant growth and success in CY23. Membership requests have steadily increased since the previous year (during which the MD-ISAC ran a small pilot program), demonstrating the continued demand for MD-ISAC's services and the value of information sharing and collaboration.

The MD-ISAC has also expanded its cyber threat intelligence (CTI) capabilities, processing thousands of CTI-based alerts/tickets in CY23. This included a wide range of alerts, such as threats to the Maryland brand identity, 3rd party leaked credential disclosures for Maryland accounts, and potential cyber threats related to State IP addresses, domains, and utilized technologies. The MD-ISAC continued to escalate potential cybersecurity findings to members and organizations within the State of Maryland’s Office of Security Management (OSM). In addition, the MD-ISAC took proactive steps to protect users from disguised cyber threats by taking down numerous malicious websites impersonating State organizations.

In addition to triaging CTI-based alerts, the MD-ISAC also published numerous Flash Alerts (FA), Advisory Reports (AR), and Threat Analyst Reports (TAR) in CY23. To complement these threat bulletins, the MD-ISAC also shared daily indicators of compromise (IOCs) /attack (IOAs) through the MD-ISAC's threat intelligence platform (TIP) to both its members and the Maryland Security Operations Center (MDSOC). These publications and daily indicators provide members with the actionable threat intelligence they need to help protect themselves from cyber threats.

Throughout CY23, the MD-ISAC CTI analysts presented several CTI-focused webinars to encourage member participation, share relevant information, and participate in Maryland Local Cybersecurity Collaborative (MLCC) meeting presentations throughout the year.

One of the highlights of the MD-ISAC's growth in CY23 was the onboarding of its first Integrator customer. This will allow the MD-ISAC's customers to automatically integrate shared intelligence with their own security tools, such as firewalls, to proactively block security threats. This, in addition to other forms of automation, will allow the MD-ISAC to continue to improve the State's ability to identify and respond to cyber threats more quickly and effectively.

Overall, the MD-ISAC has experienced significant growth and success in CY23. It has expanded its membership, improved its CTI capability, and increased proactive threat protection measures in order to better assist its members. The MD-ISAC is committed to providing its members with the information and services they need to protect themselves from cyber threats.

Additional Service Accomplishments

In addition, to the above service accomplishments, OSM is scanning more than 25,000 computers in networkMaryland and monitoring the public facing assets for all of networkMaryland continues; more than 700 log sources are being ingested and almost 4TB of information is processed daily; thirteen (13) new departments have been added to the managed vulnerability service, and OSM handled over 9,000 security incident events and remediation of more than 5,000 phishing incidents.

MLCC Successes

The Maryland Local Cybersecurity Collaborative (MLCC) was established by the Office of Security Management to enhance the cyber resiliency posture of the entire State. Comprising Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other security personnel from local jurisdictions, including counties, municipalities, and public school

systems, the MLCC serves as a platform for the Maryland cybersecurity community to convene, exchange information, and address challenges. By facilitating communication and collaboration, the MLCC aims to support the State's overarching cybersecurity mission. The Collaborative, which first convened in December 2022, provides a forum for locals to voice concerns, identify gaps, and collectively devise state-level solutions. Those interested in joining can complete the application process to participate in this initiative.

The MLCC has achieved significant milestones since its inception, garnering a membership of 174 entities, including 100% of counties, 100% public schools, many municipalities, and a few community colleges across the State. Additionally, the MLCC's membership comprises several State agencies, the legislator, federal agencies such as CISA and the FBI, and affiliate organizations and associations such as MACo, MML, MABE, Maryland TLF, MS-ISAC, and more. This extensive network underscores the Collaborative's holistic approach to cybersecurity, bringing together key stakeholders from government agencies, federal entities, affiliated organizations, and public institutions. Such inclusive membership ensures a comprehensive and well-rounded perspective in addressing cybersecurity challenges and fortifying the State's overall cyber resiliency posture.

Since its inception in December 2022, the MLCC has consistently met every other month, drawing approximately 70-90 participants to each session. The Collaborative recently marked a significant milestone with its first in-person summit in October, attracting 85 participants. Beyond these regular meetings, the MLCC has succeeded in fostering an environment characterized by sharing, collaboration, and trust. It serves as a vital platform for counties to exchange insights into both challenges and successes, contributing valuable survey responses to the State and Local Cybersecurity Grant Program (SLCGP) Committee. The Collaborative also facilitates Statewide coordination on cybersecurity matters and maintains a dedicated webpage on the Department of Information Technology (DoIT) website. This webpage serves as a valuable resource for local entities seeking information on legal requirements, available resources, and other pertinent details. Furthermore, the MLCC has innovatively introduced CISO Signal Chats, promoting communities of practice and enhancing communication among members in pursuit of a more resilient cybersecurity landscape.

The success of the Collaborative is underscored by its ability to convene stakeholders and address cybersecurity challenges on a statewide scale, making it a vital hub for promoting cyber resiliency across Maryland and fostering Maryland's steadfast commitment to cultivating a whole-of-state approach to cybersecurity.

State and Local Cybersecurity Grant Program (SLCGP)

On September 16, 2022, the Department of Homeland Security (DHS) introduced the State and Local Cybersecurity Grant Program (SLCGP), earmarking $1 billion over four years to fortify cybersecurity for state, local, territorial (SLT) governments, and tribal governments across the nation.

In the inaugural year of the grant, Maryland was allocated $3.2M, obligating 80% of funds to local entities, with 25% earmarked for rural jurisdictions. Each funding year spans a four-year "period of performance."

To meet grant requirements, Maryland formed a committee comprising state and local partners. The committee has met monthly since its inception. In addition, Maryland devised, and gained approval for the SLCGP Cybersecurity Plan. Presently, the committee is finalizing project details for submission to FEMA and CISA, seeking approval and funding for years one and two of the grants.

MABE Cybersecurity Assessments for LEAs

In 2022, Section 5 of SB754 (CH. 241, 2022), mandated all Units of Local Government in Maryland to certify compliance with the State's Minimum Cybersecurity Standards by June 30, 2023. In addition, units of local government are required to provide certification of an assessment by a third-party provider, validating the attestation.

The Maryland Board of Education (MABE) is the predominant insurance provider for the State's public school systems (Local Education Agencies, LEAs). To help LEAs meet this requirement, MABE partnered with DoIT to modify the assessment criteria and process through its existing security vendor. This initiative offers assessment services to 19 LEAs who are members of the Group Insurance Pool, aligning with both the State's Minimum Cybersecurity Standards and the assessment requisites outlined in Section 5 of SB754 (CH. 241, 2022).

Major Initiatives of 2023

In addition to the exceptional achievements outlined above, OSM teams have begun to develop new tools and services designed to provide the best in breed detection and protection capabilities. These will enable our SOC team to detect potential security events before they become a breach or major ransomware event, they will allow our security engineers to identify

with greater accuracy unsecured systems across our Statewide IT infrastructure. Together, it is technologies such as these that will further reduce the State's overall cyber risk.

Spotlight Capabilities added to MDR Service

In November 2023, OSM added a key CrowdStrike module/capability to its endpoint managed detection and response (MDR) service to support the State. This Falcon Spotlight module offers an automated, lightweight vulnerability assessment and management solution for IT analysts within Security Operations. Using Falcon Spotlight, analysts can see what vulnerabilities are exposed within their environments and prioritize them. Further, they can manage patch processes, conduct emergency patches for critical hosts and create custom dashboards to filter for priority vulnerabilities to expedite remediation. By using the same Falcon agent and cloud technology, scans become continuous and are always up to date, while the impact to endpoints is eliminated. Seamless integration with OSM's other modules means analysts can quickly pivot between vulnerability information, incident details, and endpoint activities, both historically and in real time.

Cybersecurity Asset Attack Surface Management (CAASM)

In December 2023, OSM procured a Cybersecurity Asset Attack Surface Management (CAASM) solution. This solution can provide OSM with a consolidated inventory of IT assets, eliminating debates over asset presence, patch status, and security tool coverage. This capability will develop over the course of early 2024.

Centralized Logging Solution

OSM has recently procured a centralized logging solution to support the significant improvements to the cyber environment for the State as it's essential for OSM to be prepared to receive important security logs from non-enterprise units of State Government. This simplifies the process, allowing OSM to smoothly integrate these vital logs into their central SIEM without disrupting the external organization's environment. Additionally, it gives OSM the flexibility to expand log storage without increasing licensing costs. It also provides the option to store raw logs outside the Security Information and Event Management (SIEM), which is cost-effective and enables selective retrieval as needed, such as for incident response and other specific requirements.

Cybersecurity as a Team Sport

Cybersecurtiy is not a technical function that occurs in a vacuum, or data center behind closed doors. Security touches nearly every aspect of IT and the overwhelming majority of business processes. While technology is important to implementing a robust information security program, it is the people who ensure security is carried out in all aspects of State government operations. People are our most valuable asset in combating cyber-attacks. It is our people that we need to ensure are always on high alert for abnormal behavior of applications, websites, mobile devices, as well as other people. Cybersecurity relies on the reporting by our users to quickly respond to malicious events. To this end, security awareness training and other educational resources are critical to a successful security program.

Statewide Cybersecurity Training Program

The Maryland Department of Information Technology (DoIT) Office of Security Management (OSM) continued its partnership with the Maryland Department of Labor for the Cybersecurity Operational Methods Education Training (“COMET”) training program via the Employment Advancement Right Now (EARN) Maryland program grantee BCR Cyber. BCR Cyber provided cutting edge cybersecurity training to over 100 Maryland State government employees in 2023, totaling over 150 State employees trained to date. This Statewide training consisted of both Incumbent (CompTIA Security+ certification) and Advanced Incumbent Training Certified Information Security Systems Professional Certification (“CISSP”).

October Cybersecurity Awareness Month (OCSAM)

To promote October Cybersecurity Awareness Month (OCSAM), DoIT OSM engaged State agencies in key cyber topics, and released cyber training and awareness related communications, videos, tips, and important cyber hygiene reminders throughout the month of October for all State employees and contractors. There were over 1,800 website views during the month, and over 400 people attended the Cybersecurity Awareness lunch and learn held by OSM in late October 2023.

Closing Statement

OSM appreciates the opportunity to provide this Year in Review for 2023 and continues to strive to improve the State's cybersecurity posture. OSM will continue to focus on developing and executing the State’s cybersecurity strategy, in partnership with the State Legislature, Executive Leadership, and the Governor of the State of Maryland.