Office of Security Management

Cybersecurity 2022
Year in Review

Contents

Securing Technology, Today and Tomorrow

Message from the State Chief Information Security Officer

Dear Cybersecurity Team,

Continuing the tradition we started last year, I'm pleased to share the "Office of Security Management - Cybersecurity 2022 - Year in Review." When we published last year's retrospective, I recognized that team's accomplishments established a seemingly unattainable expectation of achievement. Unsurprisingly, the groups that constitute the Office of Security Management delivered a massive list of accomplishments once again. This report details many of the wonderful activities and achievements of the year.

While our accomplishments around it are described in detail later in this report, an issue that I am particularly passionate about is workforce development. This year, that list includes everything from growing the capabilities of the State's many cybersecurity professionals to creating a roadmap for IT workers to become partners or members of the cybersecurity teams. I'm hopeful that soon, we'll be able to create pathways into IT and cybersecurity careers for interested State employees, regardless of their current skillset or assignment.

Much of our success is because one of our guiding principles is that "Cybersecurity is a team sport." For us, that means everyone is part of that team, regardless of their role. This approach is the only pathway to success.

With that, I would like to offer a sincere thank you to everyone for doing their part to keep Maryland secure!

Charles "Chip" Stewart
State Chief Information Security Officer

Session 2022 – Legislative Update

Legislative impact on Statewide Cybersecurity

This year, we saw several cybersecurity-focused bills progress through the legislative process and get signed by the Governor. These bills reflect the confidence of the legislative and executive branch leadership in the Office of Security Management's ability to defend against cyberattacks and help the whole State prepare, respond, and recover from cyber disruptions.

While some of the content within these bills codified the cybersecurity measures implemented by executive order, they expanded the authorities of the State Chief Information Security Officer and the Office of Security Management. In addition, these bills went on to strengthen the State-Local partnerships and to codify a group that helps to influence the State's technology investment decisions. Through the diligent work of the Department of Information Technology, Department of Emergency Management, and the Office of Security Management, many of the requirements established in these legislative packages are fully implemented, or the team is well on its way to implementing.

Governor Hogan signing Senate Bill 754 into Law

Legislative Implementation Status

Requirement	Ch. 241	Ch. 242	Ch. 243	Status
Hire a Director of State Cybersecurity		X		Complete
Hire a Director of Local Cybersecurity		X		Complete
Conduct Quarterly MCCC Meetings		X		Complete
Establish State cybersecurity incident reporting requirements		X		Complete
Establish local cybersecurity incident reporting requirements	X			Complete
Establish guidelines on cybersecurity incident disclosure		X		Complete
Implement a Statewide GRC Platform		X		Complete
Create Statewide Cybersecurity Strategy		X		Ongoing
Create MD-ISAC	X			Complete
Commission a feasibility study for expanding the SOC	X			Ongoing

Chapter 242 - State Government – Cybersecurity – Coordination and Governance

Senate Bill 812
Senators Hester, Hershey, Jennings, Jackson, Rosapepe, Lee, and Watson

Cross-filed with House Bill 1346
Delegates P. Young, Kerr, Bartlett, Kelly, Bagnall, Bhandari, Carr, Chisholm, Cullison, Hill, Johnson, Kaiser, Kipke, Landis, R. Lewis, Morgan, Pena-Melnyk, Pendergrass, Reilly, Rosenberg, Saab, Sample-Hughes, Szeliga, and K. Young

This bill significantly expands and enhances the State's regulatory framework for State and local government cybersecurity. Among other things, the bill:

1. codifies and expands the Maryland Cyber Defense Initiative including creating the positions of director of State and Local Cybersecurity;
2. establishes various assessment and reporting requirements for State agencies and local governments;
3. requires the Department of Information Technology (DoIT) to ensure each agency's compliance with cybersecurity standards under certain circumstances; and
4. requires DoIT to develop a centralization transition strategy and conduct a self-performance and capacity assessment.

The Governor must include an appropriation in the annual budget bill in an amount necessary to cover the costs of implementing a required statewide cybersecurity master plan without the need for DoIT to operate a charge-back model for cybersecurity services provided to units of State and local government. For fiscal 2023, funds may be transferred by budget amendment from the Dedicated Purpose Account (DPA) to implement the bill.

Chapter 241 - Local Government Cybersecurity – Coordination and Operations

Senate Bill 754
Senators Hester, Hershey, Jennings, Jackson, Rosapepe, Lee, and Watson

Cross-filed with House Bill 1202
Delegates P. Young, Kerr, Feldmark, Bartlett, Kelly, Kipke, Ebersole, Hornberger, McIntosh, Bagnall, Bhandari, Carr, Chisholm, Cullison, Hill, Johnson, Kaiser, Landis, R. Lewis, Morgan, Pena-Melnyk, Pendergrass, Reilly, Rosenberg, Saab, Sample-Hughes, Szeliga, and K. Young

This emergency bill makes numerous changes to the State's cybersecurity infrastructure, practices, and procedures, primarily for local governments, by, among other things,

1. codifying (in part) and expanding the executive order that established the Maryland Cyber Defense Initiative;

2. establishing the Cybersecurity Preparedness Unit in the Maryland Department of Emergency Management (MDEM) and the Information Sharing and Analysis Center (ISAC) within the Department of Information Technology (DoIT);
3. requiring specified local government entities to create or update cybersecurity preparedness and response plans and complete cybersecurity preparedness assessments, as specified;
4. requiring DoIT to provide guidance to local governments to bring their cybersecurity practices into compliance with cybersecurity standards.

For fiscal 2023, funds from the Dedicated Purpose Account (DPA) may be transferred by budget amendment to implement the bill. Beginning in fiscal 2024, the Governor must include in the annual budget bill specified funding for staff for the Cybersecurity Preparedness Unit.

Chapter 243 - State Government – Information Technology and Cybersecurity–Related Infrastructure (Modernize Maryland Act of 2022)

House Bill 1205
Delegates P. Young, Kerr, Feldmark, Bartlett, Kelly, Kipke, McIntosh, Bagnall, Bhandari, Carr, Chisholm, Cullison, Hill, Johnson, Kaiser, Landis, R. Lewis, Morgan, Pena-Melnyk, Pendergrass, Reilly, Rosenberg, Saab, Sample-Hughes, Szeliga, and K. Young

Cross-filed with Senate Bill 811
Senators Hester, Corderman, Eckardt, Edwards, Elfreth, Griffith, Jackson, King, McCray, Rosapepe, Salling, Young, and Zucker

This emergency bill establishes an independent Modernize Maryland Oversight Commission to:

1. Ensure the confidentiality, integrity and availability of information held by the State
2. Advise the Secretary of Information Technology and the State Chief Information Security Officer (SCISO) on appropriate IT and cybersecurity investments and upgrades, funding sources, and future procurement mechanisms, as specified.

DoIT must also hire independent contractors to develop a framework for investments in technology, and according to that framework, once at least every two years, the department must assess the cybersecurity and IT systems for each unit of State government. The framework must include specified criteria, and each affected unit of State government must promptly provide the contractors with the information necessary to perform the assessments. Every two years, the contractors must provide the results of the assessments to the Modernize Maryland Oversight Commission and specified committees of the General Assembly.

The Bill also expands cybersecurity requirements for State agencies and water and sewer systems, and makes related changes to cybersecurity infrastructure funding and

procurement by the State and local governments. For fiscal 2023, funds from the Dedicated Purpose Account (DPA) may be transferred to implement the bill. For fiscal 2024, the Governor must include in the annual budget bill an appropriation of at least 20% of the aggregated amount appropriated for information technology (IT) and cybersecurity resources in the annual budget bill for fiscal 2023.

Major Cyber-Accomplishments of 2022

Statewide Cybersecurity Tabletop Exercise

On October 27, 2022, the State Chief Data Officer, State Chief Privacy Officer, and State Chief Information Security Officer conducted the first Statewide Cybersecurity Tabletop Exercise in collaboration with partners at the Maryland Department of Emergency Management. Starting with a workshop, agency executives and technical leadership learned about many active threats, considerations for responding to and communicating about cybersecurity incidents, and the threat actors that are perpetrating these crimes.

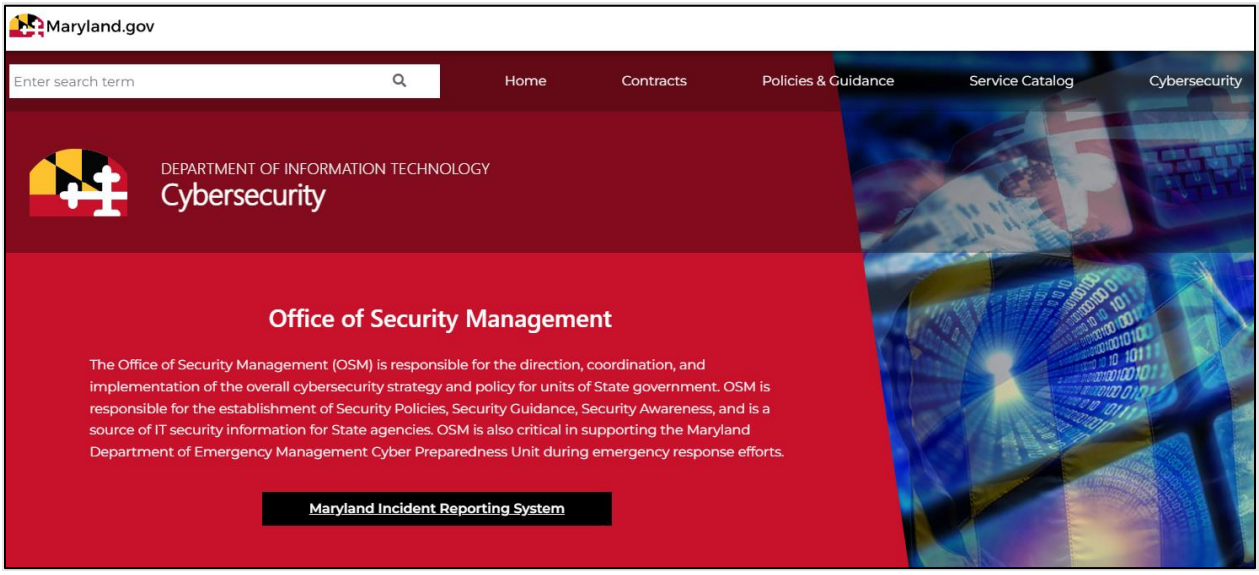
Members of the executive branch during the workshop on incident response and communication.

The session culminated with a “Tabletop Exercise” that simulated a substantial cybersecurity incident impacting multiple agencies and business functions. There was a focus on how the State would respond to an incident and how to communicate the incident and recovery actions to employees, partners, and citizens. This exercise helped prepare agencies for the soon-to-be-established “Centers of Excellence” within the Office of Security Management, focused on Incident Response, Disaster Recovery, and Technology Business Continuity.

Spreading the Cyber-Word

Dedicated Cybersecurity Webpage

Cybersecurity communications are vital to ensuring employees and constituents are aware of any emerging threats and establishing directives for protection. A mechanism for OSM communication is critical to provide any new or readily available information to its consumers. The Cybersecurity webpage, accessible from the header of the DoIT website, went live in October 2022 to communicate various cybersecurity information to the State. Useful policies, guidance, links, cyber-related reports, bulletins, and information are currently on the site. The team is constantly adding press releases, standards, policies, and guidance to the new site, available at https://doit.maryland.gov/cybersecurity/.



In addition to news and other press releases, the website contains several other artifacts required as part of the 2022 legislative packages, including:

- Cybersecurity Incident Reporting Requirements for Local Governments
- Cybersecurity Incident Reporting Requirements for State Government
- Minimum Security Standard for Units of Government on networkMaryland
- Guidelines for the Public Disclosure of Cybersecurity Incidents

Aligned with the requirement to establish standards for reporting cybersecurity incidents, the Office of Security Management launched the “Maryland Incident Reporting System,” an online portal for reporting cybersecurity incidents directly to the Maryland Security Operations Center. The Maryland Incident Reporting System is available from the cybersecurity web page and directly at https://doitmaryland.service-now.com/cybersecurityincident/.

Binding Operational and Emergency Directives

While a single policy would not typically be worthy of a heading in a year-end retrospective, Maryland is leading the way by establishing a policy that grants the State Chief Information Security Officer the ability to issue strategic and tactical directives. This capability mirrors those assigned to the Cybersecurity and Infrastructure Security Agency (CISA) in helping to protect the nation. In December of 2022, following strong warnings from our federal partners, the State Chief Information Security Officer issued the first emergency directive to help protect State systems from foreign governments by establishing a prohibited products list, including the popular social media application "TikTok," from being installed on State systems.

Maryland Cybersecurity Coordinating Council

The legislature significantly expanded Maryland Cybersecurity Coordinating Council (MCCC) membership in the 2022 legislative session. The membership now consists of Secretaries or designees from every principal department in the executive branch.

The council holds meetings at some of Maryland's flagship business partners' facilities. This approach exposes MCCC members to some of the great cybersecurity partners of the State while providing the general public an opportunity to see some of the great work these businesses are doing.
The MCCC held two exceptionally well-attended meetings this year at the Baltimore Cyber Range and the DreamPort facility in Columbia, MD, and is looking forward to exciting locations in 2023!

One of the highlights of the tour of DreamPort for the MCCC members was the miniature "Smart City" that allows cybersecurity simulations on real operational technology.

Maryland Local Cybersecurity Collaborative

Recognizing the diverse needs of the many partners in our State, the Maryland Local Cybersecurity Collaborative (MLCC) was created by the Office of Security Management as part of the initiatives to achieve a "whole of state" cyber resiliency posture. Led by the Director of Local Cybersecurity, the MLCC brings CIOs, CISOs, and other security personnel from the many local jurisdictions across the State, such as counties, municipalities, and public school systems.

The goal of the MLCC is to create a space where the Maryland cybersecurity community can meet, get information, and share information. The MLCC will also provide an avenue to foster the State's mission to improve "whole of state" cybersecurity by promoting an environment for local jurisdictions to express their challenges and needs, identify gaps, and think of State-level

solutions to support the locals. Locals will also be recipients of vital intel, kept abreast of new legislation and requirements, and have a place to share resources and training opportunities.

The MLCC had its inaugural meeting in December of 2022 and will meet every other month.

Major Initiatives of 2022

Cybersecurity Assessments and Remediation

An essential part of minimizing cybersecurity-related risk is conducting assessments of the maturity of the capabilities, policies, and technology that protect organizations. The Statewide Cybersecurity Assessment Program kicked off in mid-2021 and concluded its first phase in mid-2022. Over 75 agencies/units across the State had cybersecurity maturity assessments performed using the NIST Cybersecurity Framework (CSF). In addition, the team conducted more than forty external penetration tests that validated the security control implementation of the agency's external IT systems.

The maturity assessment provided a high-level analysis of current practices and gaps, with the ability to prioritize and address those. The penetration tests identified weaknesses in application and organizational boundaries for unauthorized access mechanisms, and visibility into the issues with configurations and system lifecycle. As with many of our other successful initiatives, the legislature included this as a periodic activity in law. Starting in 2023, these cybersecurity assessments will be performed every two years.

Some common themes included the assurance of accurate and critical IT asset inventory, a lack of digital identity and processes, the need for developed and updated business continuity/disaster recovery and incident response plans, and modern endpoint detection.

In addition to the NIST CSF assessments, the Office of Security Management engaged in two additional evaluation projects. First, an independent third party conducted a tactical and strategic gap analysis of security operations at the request of the State Chief Information Security Officer. Additionally, an independent third party conducted a performance and capacity assessment of the entire Office of Security Management due to the legislative requirements.

Based upon the assessments that the team completed in 2022 and the resulting Statewide remediation roadmap, several cybersecurity improvement initiatives began in late 2022 and will continue throughout 2023 and beyond to ensure Maryland maintains a strong cybersecurity foundation. Some of the transformational remediation projects include:

Agency Information Security Officer Program
Creating the governance, hiring and performance materials, and tasking to embed executive cybersecurity talent within every agency.

Statewide Endpoint Detection and Response Platform
Deploying a scalable Statewide Endpoint Detection and Response capability that integrates with the Maryland Security Operations Center to protect the IT assets from common and advanced threats.

Security Training Program: Usability Improvement
Improving the usability of the security training and awareness service by building and communicating service and performance metrics for each agency, making the service easier to use for agencies, and improving the non-visual accessibility of the training content.

Security Training Program: Role-Based Training
Developing role-based training programs better prepare the various types of users and job functions for their specific threat profiles.

Centers of Excellence - Disaster Recovery, Business Continuity, Risk Management, and Incident Response
Creating an internal capability with the tools, templates, and training to support agencies and local governments in developing the plans, policies, and proficiencies for these critical cybersecurity needs.

Security Operations Center Maturation Initiatives
Improving the governance, capabilities, and operations of the Maryland Security Operations Center by establishing governance documents, formalizing the processes and procedures used by the team, and developing metrics to ensure the service meets its performance objectives.

Maryland Information Sharing and Analysis Center (MD-ISAC)

One of the most exciting achievements of 2022 is the official instantiation of the Maryland Information Sharing and Analysis Center (MD-ISAC). By design, the MD-ISAC is the hub for sharing bidirectional strategic and tactical Cyber Threat Intelligence for Maryland governments, whether they are State agencies, counties, municipalities, school systems, universities, or any other political subdivision. Cyber Threat Intelligence, often called CTI, is one of the biggest force multipliers that enables cyber teams to defend against cyber-attacks.

The MD-ISAC aims to produce timely, relevant, actionable cyber threat intelligence that meets the common needs across the breadth of state and local government stakeholders to reduce cyber risk. Cyber-attacks present challenges for agencies that must defend their data and systems from capable threat actors. Given the risks that these threats present, it is increasingly important that agencies share cyber threat information and use it to improve their security posture. The core of the MD-ISAC is the Anomali information sharing & analysis center (ISAC) platform, which collects and delivers threat information to the internal CTI team. The CTI team analyzes the threat information and prepares it for sharing across customer agencies. Sharing

methods include threat bulletins, Indicator of Compromise/Attack reports (ICAR) via email, and a self-service CTI library. By exchanging cyber threat intelligence within a collaborative community, agencies can leverage that group's collective knowledge, experience, and capabilities to understand the threats they face.

Beyond information about threats, the MD-ISAC team, in coordination with the vulnerability management team, is engaged in activities to minimize our collective attack surface. Our attack surface is the sum of the assets accessible to cyber criminals where vulnerabilities exist. The team does this using several sources of vulnerability and attack surface intelligence, including Shodan and Palo Alto Expanse. With these tools, the team can help reduce the likelihood that a cybercriminal can exploit a vulnerability, helping to reduce risk further.

By aggregating this capability inside the Maryland Security Operations Center (MD-SOC), we have developed a robust and advanced capability that allows us to capitalize on the economy of scale that only the State can achieve. While some components of this program were started in 2021, this year saw a significant maturation and formalization of the program into what vendors and partners describe as a model for other states.

MD-ISAC membership is open to all government entities within the State, including counties, cities, towns, and public school systems. For more information about signing up, these entities should contact the MD-ISAC by emailing md-isac@maryland.gov from their official government email address.

Directors of State Cybersecurity and Local Cybersecurity

As part of an overarching cybersecurity legislative package passed early this year, the Office of Security Management has hired a Director of State Cybersecurity and a Director of Local Cybersecurity. These foundational leadership roles will support the vision for "Whole of State Cybersecurity."

Governor Hogan with Director of Local Cybersecurity, Netta Squires, and John Bruns, Director of State Cybersecurity.

By dedicating resources to building relationships with local governments, the State can help provide resources to reduce the likelihood of successful cyberattacks against local governments, and that local governments are positioned to get the assistance they need in the event of a successful cyberattack. To achieve this goal, the Director of Local Cybersecurity works in coordination with the Maryland Department of Emergency Management to provide assistance and improve cybersecurity preparedness throughout the counties and municipalities across the State.

Similar to the Director of Local Cybersecurity, the Director of State Cybersecurity works directly with executive branch agencies to help solidify and secure the State executive branch's information technology systems and data. He also assists the State Chief Information Security Officer in developing and maintaining information technology security policy and guidance that is standardized across all state agencies.

The Director of State Cybersecurity, John A. Bruns, has over 15 years of experience developing, managing, and delivering mission-critical IT security, application, and infrastructure projects for government and corporate clients. Mr. Bruns was previously the Chief Information Security Officer (CISO) for Howard County Government. There, he developed risk-based cybersecurity strategies and policies, collaborating with the Chief Information Officer and the County Executive to implement security prevention, detection, and response across much of Howard County Government infrastructure. Before his role as Howard County CISO, John served as a consultant in multiple positions for the Maryland State Department of Education.

The Director of Local Cybersecurity, Netta Squires, Esq., has over 14 years of experience in emergency management and incident response and almost seven years of specific expertise in cybersecurity. She previously worked as an Emergency Management Specialist for the Montgomery County Office of Emergency Management and Homeland Security. There, she managed multiple projects and teams in various emergency support functions. Ms. Squires has her Juris Doctorate from George Washington Law School and a Master of Science in Law in Cybersecurity from UMB School of Law. She is also a Certified Emergency Manager (CEM) by the International Association of Emergency Managers. Additionally, she works with the

Governor's Subcabinet on Infrastructure to help administer the cybersecurity portion of funding from the federal "Infrastructure Investment and Jobs Act" (IIJA) to local communities.

Both directors work in the Office of Security Management within the Department of Information Technology and report to the State Chief Information Security Officer.

New Services and Capabilities

Statewide GRC Platform: ServiceNow Integrated Risk Management (IRM)

In a continued effort to establish a mature, statewide Governance, Risk, and Compliance (GRC) program, the Department of Information Technology's Office of Security Management implemented ServiceNow's Integrated Risk Management platform to allow for the effective execution of statewide agency NIST Cybersecurity Framework assessments. The platform will allow for tracking of agency assessments, key risk indicators, issue remediation, and reporting across calendar years. In addition, the ServiceNow IRM Pro platform offers a centralized system to conduct system Authorization to Operate (ATO) assessments for critical enterprise, statewide services managed by DoIT. Moving forward, the Director of Governance, Risk, and Compliance (GRC) will be responsible for the continued success and implementation of the GRC program.

Statewide Managed Detection and Response (MDR)

In November 2022, the State of Maryland procured Crowdstrike's Endpoint Detection and Response platform, enabling a new, cutting-edge security approach that addresses endpoint protection, detection, and response on workstations, laptops, mobile services, and servers. The DoIT Office of Security Management has dedicated significant planning and resources to develop a Statewide Managed Detection and Response (MDR) service with hands-on, 24/7/365 response and remediation of cybersecurity incidents supported by the Maryland Security Operations Center staff and the Crowdstrike Falcon Complete Team. In the first quarter of 2023, DoIT OSM anticipates the onboarding of DoIT's enterprised agencies, the Maryland Department of Health, Department of Human Services, MDTHINK, Comptroller, DLS OLA, OAH, OPD, and the Maryland Health Business Exchange. All state agencies have been encouraged to replace legacy endpoint protection platforms and antivirus over the 2023 year with the new MDR service. DoIT OSM will continue to host training for SOC analysts and administrative users via Crowdstrike University.

Cybersecurity as a Team Sport

Equipping all State Employees to contribute to the State's cyber-mission

Governor Hogan presented State CISO Chip Stewart with a proclamation declaring October as Maryland's Cybersecurity Awareness Month.

Nearly every State employee, contractor, and vendor contributes to the defense of our computer systems. Whether using our email service, state systems to conduct business, or connecting their systems to ours, we are collectively responsible for keeping the State secure.

That is why we, as a State, continue to invest in building a robust and diverse talent pipeline. The Office of Security Management is sourcing entry-level talent from traditional sources such as internships while also moving forward to engage with individuals who would typically be passed over for opportunity, using the State's new "Innovative Workforce" apprenticeship contract.

But expanding the pool of talent doesn't stop there. Through the relationship formed during the first meeting of the new Maryland Cybersecurity Coordinating Council, there is an ongoing effort to bolster the State's incumbent Information Technology and Cybersecurity workforce with no cost to the employee training and certification opportunities.

Cybersecurity Awareness and Training

OSM continues to enhance our statewide cybersecurity awareness training program via the Infosec IQ platform to include role-based training. Role-based training tailors the training to fit the roles of the staff and highlights the security risks associated with those roles. As part of this initiative, users with advanced access privileges or access to sensitive data (e.g., HIPAA, PCI, FTI, CJIS, FERPA, PII) will be assigned role-based training. Role-based training (RBT) will occur upon agency onboarding, for new hires during onboarding activities, and annually after that. The team completed the pilot rollout in early December 2022, and we anticipate statewide agency rollout will start in early 2023.

Additionally, the OSM security awareness training team monitors and tracks statewide agency training compliance. The team is conducting meetings with agency-assigned training managers to collaborate on ways to improve completion rates, ensure the accuracy of the training roster, and make continuous improvements to the program.

Internship Programs

Once again, in partnership with UMBC, the Office of Security Management has continued to promote entrance into the cybersecurity workforce through the Maryland Technology Internship Program (MTIP) and the Maryland Institute for Innovative Computing (MIIC) internship programs. Through this program, the Office of Security Management continues to have tremendous success converting team members from interns to permanent staff.

The Board of Public works recognized interns participating in the MTIP and MIIC programs on August 10, 2022.

Statewide Cybersecurity Training Initiative (Cyber Range)

In partnership with the Maryland Department of Labor and the Baltimore Cyber Range, the OSM team is coordinating the cybersecurity training and certification opportunity for 100 State employees. With funding from the Employment Advancement Right Now (EARN) Maryland program, a grant program administered by the Maryland Department of Labor, this training will positively impact the State workforce by both teaching various skill levels of IT and cybersecurity experience several key cybersecurity practices and allowing the opportunity for 50 state employees to take the Certified Information Security Systems Professional (CISSP) exam. Employees have been enthusiastic about the opportunity to attend such training in the State at no cost to them. The first training session kicked off in early December 2022, and the second will start in February 2023.

The re-formed Maryland Cybersecurity Coordinating Council held it's first meeting at the Baltimore Cyber Range.

Looking Forward - Roadmap for 2023

Transition and Briefings

As we prepare to support the transition of administrations, we look forward to ensuring a smooth and secure transition. Because transitions create opportunities for cybercriminals to take advantage of gaps in coverage, the Office of Security Management is operating on the highest alert level. We have briefed the incoming administration on the status of cybersecurity in Maryland and are confident that they will continue to make cybersecurity a strategic and tactical priority.

Local Government Collaboration

As we look forward to 2023, we expect that the Infrastructure Investment and Jobs Act (IIJA) State and Local Cybersecurity Grant Program (SLCGP) will encourage more collaboration with local government partners.

Between the “Centers of Excellence” in the Statewide cybersecurity remediation project, the further rollout of the MD-ISAC, and everything in between, we expect the relationships with the local governments across the State to flourish.

Service Improvement

Statewide Crisis Communications Platform
The Office of Security Management is working in collaboration with the Department of Information Technology’s IT teams and the Department of Emergency Management to gather requirements and implement a Statewide crisis communications platform. Successful implementation of this platform will facilitate real-time updates to employees regarding cybersecurity incidents, flash awareness bulletins, or IT outages.

Annual Service Summits
Gathering feedback from our customers on any unmet cybersecurity needs, service performance, and what we see for the future of cybersecurity in Maryland. We’re planning the first to be on “Cybersecurity Awareness and Training” in the first quarter of 2023.

We look forward to having you on Maryland’s Cybersecurity Team!