STATE CYBERSECURITY CENTRALIZATION STRATEGY

JULY 2023

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary
Melissa Leaman | Deputy Secretary

TABLE OF CONTENTS

1. Introduction

There has never been a more opportune moment in the state's history for Maryland's Executive Branch to work together and promote the collective defense and resilience of our technologies, networks, systems, and data. Emerging trends noted by the National Cybersecurity Strategy include the ever-growing complexity and interconnectivity of software and systems used by our state's employees, constituents, and businesses that access the global internet, presenting a significant risk to our government's critical infrastructure and essential services that must be actively protected through strategic planning, investment, and collaboration[1].

To safeguard Maryland's Executive Branch Government's information technology infrastructure, the State Cybersecurity Centralization Strategy addresses key challenges, including:

1. **Disparate Operations and Toolsets:** Streamlining and standardizing operations and toolsets enhances efficiency and effectiveness.
2. **Lack of Visibility Across Atomized Networks:** Comprehensive network visibility is essential for identifying and mitigating potential threats.
3. **Ever-Growing Telemetry:** We recognize the importance of harnessing telemetry data from on-premise, cloud, and remote systems to enhance threat detection capabilities.
4. **Limited Cybersecurity Budgets:** Despite budget constraints, we will maximize the impact of available resources through prudent prioritization.
5. **Competitive Job Market for Security Talent:** Attracting and retaining skilled security professionals is a priority, and we will provide competitive opportunities to nurture talent.
6. **Lack of Collaboration and Trust Between Organizations:** Fostering a culture of collaboration and trust will enable strong partnerships for collective defense.
7. **Continued Increase in State-Sponsored Advanced Persistent Threats (APTs):** To combat sophisticated threats, we will enhance our cyber resilience measures through proactive defenses.

With the mission to detect incidents in seconds, respond in minutes, and remediate in under an hour, the Maryland Security Operations Center (MDSOC) and the Maryland Information Sharing and Analysis Center (MD-ISAC) under the Maryland Department of Information Technology (DoIT) Office of Security Management (OSM) must be empowered to defend networks, systems, and users. The MDSOC and MD-ISAC must have full

[1] Office of the National Cyber Director. *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

visibility of the entire Executive Branch attack surface, including all internal and external users and systems. By leveraging integrated technologies, centralized logging, advanced threat intelligence, expert threat hunting, and highly trained incident responders, the Maryland Government Executive Branch will be prepared to respond quickly and vigilantly to improve the state's cyber readiness and resilience.

The State Cybersecurity Centralization Strategy is designed to overcome these challenges and fulfill the mission of DoIT OSM, MDSOC and MD-ISAC. It provides key recommendations for centralizing all cybersecurity planning, policies, metrics, technologies, tools, staffing, and incident response capabilities. Additionally, the strategy addresses the requirements of Senate Bill 812 (SB812) by offering recommendations related to cyber training, budget, metrics, logging, and staffing.

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.

2. Purpose

In accordance with Section 5 of SB812, Ch. 242 (2022),[2] 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[3]," and
2) "Serve as the basis for budget allocations for cybersecurity preparedness for the Executive Branch of State Government[4]."

As the entity responsible for directing, coordinating, and implementing the overall cybersecurity strategy and policy across State Government units, DoIT OSM presents the following key recommendations:

- Strengthen Incident Response capabilities,
- Centralization of Operational Logs to the MDSOC,
- Security Improvement Dashboards to inform budgetary appropriations,
- Development of Consistent Performance Accountability Metrics for Information Technology and Cybersecurity Staff, and
- Addition of Staff or Contractors required to carry out DoIT OSM duties.

To ensure transparency and accountability, the strategy and recommendations formulated under the State Cybersecurity Centralization Strategy will be duly reported to the Governor, the "Senate Education, Health, and Environmental Affairs Committee," and the "House Health and Government Operations Committee."

[2] Maryland SB0812, 2022, https://mgaleg.maryland.gov/2022RS/bills/sb/sb0812E.pdf.

[3] Ibid.
[4] Ibid.

3. Acronyms

The following acronyms and definitions apply to this document:

- BAS - Breach and Attack Simulations
- CASB – Cloud Access Security Broker
- CISA - Cybersecurity and Infrastructure Security Agency
- CISSP - Certified Information Systems Security Professional
- CMDB - Configuration Management Database
- CoE - Centers of Excellence
- CSIRT - Cybersecurity Incident Response Team
- CTI - Cyberthreat Intelligence
- DFIR - Data Forensics and Incident Response
- DHS - Department of Homeland Security
- DoIT - Department of Information Technology
- DLP – Data Loss Prevention
- DNS – Domain Name System
- DPA – Dedicated Purpose Account
- EDR - Endpoint Detection and Response
- GRC - Governance Risk and Compliance
- HAM - Hardware Asset Management
- HVAs - High-Value Assets
- IDS – Intrusion Detection System
- IDPS – Instruction Detection and Prevention System
- IoAs - Indicators of Attack
- IoCs - Indicators of Compromise
- IPS – Intrusion Prevention System
- IR - Incident Response
- ISO - Information Security Officer
- ITDR - Identity Threat Detection and Response
- ITP - Identity Threat Protection
- KPIs - key performance indicators
- MD-ISAC - Maryland Information Sharing and Analysis Center
- MDSOC - Maryland Security Operations Center
- ODMs - Outcome Driven Metrics
- OSM - Office of Security Management
- SaaS - Software as a Service
- SIEM - Security Incident and Event Management
- SLA - Service Level Agreements
- SOAR - Security Orchestration and Automated Response

- SSE – Secure Service Edge
- SWG – Secure Web Gateway
- TTXs - Table Top Exercises
- UEM - Unified Endpoint Management
- VDI - Virtual Desktop Interface
- VPN – Virtual Private Network
- ZTNA – Zero Trust Network Access

4. Improving Incident Response

To bolster the state's capability in centrally providing incident response, several key measures must be taken. This includes the establishment of leadership, policies, plans, procedures, and playbooks that contribute to effective incident handling (investigation, analysis, triage, containment, eradication, and remediation). In addition, emphasis on incident response training, tabletop exercises, attack emulation, threat hunting, efficient communication, and incident closure are crucial components of this measure.

The following improvements represent both achievements and recommendations to further the development and efficacy of incident response across the Maryland Government Executive Branch:

1. **Leadership Empowerment:** Assigning dedicated leadership with clear authority and responsibility for incident response operations will ensure a coordinated and effective response to potential cyber threats.
2. **Robust Policies and Plans:** Developing comprehensive and up-to-date incident response policies and plans that align with industry best practices will provide a solid framework for handling various cyber incidents.
3. **Efficient Procedures and Playbooks:** Streamlining incident response procedures and creating detailed playbooks tailored to specific threats will facilitate swift and consistent response actions.
4. **Continuous Incident Response Training:** Regular training programs for incident responders will ensure that personnel are well-prepared to handle evolving cyber threats effectively.
5. **Realistic Tabletop Exercises:** Conducting regular tabletop exercises that simulate real-world scenarios will enhance the preparedness of the incident response team and foster effective collaboration between different departments.
6. **Effective Attack Emulation:** Performing controlled attack simulations in a safe environment will help assess the organization's defensive capabilities and identify areas for improvement.
7. **Proactive Threat Hunting:** Implementing proactive threat hunting practices will enable the early detection and mitigation of potential threats before they escalate.
8. **Efficient Communication Protocols:** Establishing clear communication protocols within the incident response team and with relevant stakeholders will ensure smooth information sharing during critical incidents.
9. **Timely Incident Closure:** Developing well-defined criteria for incident closure and conducting thorough post-incident analysis will aid in continuous improvement and learning from past incidents.

4.1 Creation of the Director of Cyber Resilience

In June 2023, DoIT OSM, under the leadership of Secretary Katie Savage, took significant strides in enhancing Maryland's cybersecurity posture by creating a pivotal position – the Director of Cyber Resilience. This accomplished professional was diligently selected to oversee and lead the MDSOC, assuming responsibility for a wide array of critical systems and functions. These include managing the Security Information and Event Management (SIEM) solution, Security Orchestration and Automated Response (SOAR), incident response plan and playbook creation, data forensics, SOC performance monitoring, SOC training, security incident ticket handling, and threat hunting. Additionally, the Director of Cyber Resilience was entrusted with spearheading the attack emulation program and driving efforts to fortify the Centers of Excellence (CoE), which serve as vital resources for disaster recovery and business continuity improvement.

Essential job functions for the Director of Cyber Resilience will include oversight and management of Maryland's 24/7 SOC team and Cybersecurity Incident Response Team (CSIRT). In addition, the Director will develop and execute an attack emulation program that goes beyond traditional penetration testing and integrates purple teaming tools and techniques, providing the state with the capability of performing both red teaming offensive exercises and blue team defense exercises. The Director of Cyber Resilience will also serve as the CSIRT Incident Commander during cybersecurity incident response exercises, helping to design and develop effective tabletop exercises (TTXs) to help establish and improve communication lines between internal and external partners, as well as practice following the state's cybersecurity incident response plans and procedures.

4.2 Establishment of Incident Response Services

To enhance incident response capabilities across all units of the Executive Branch, DoIT OSM continues to develop comprehensive services designed to address a wide range of cybersecurity incidents. Basic services provided by the MDSOC include handling all incidents submitted through various channels such as email, phone, or internal ticketing systems. The MDSOC also provides a 24/7 call center with hands-on-keyboard response, ensuring immediate assistance during critical situations.

DoIT OSM recommends further strengthening the incident response team by leveraging Tier 1 (T1), Tier 2 (T2), and Tier 3 (T3) SOC Analysts, including skilled digital forensics investigators. To complement these internal resources, strategic partnerships with external vendors are encouraged to offer the following services to the Executive Branch:

- **Incident Response Retainer:** Incident Response (IR) Retainers allow skilled cybersecurity experts to provide fast, on-site response in the event of an incident or data breach of a magnitude that requires support across leadership, operations, and security teams. Often, IR retainers are obtained via 3rd party insurance providers or from expert Data Forensics and Incident Response (DFIR) companies. DoIT OSM should offer a dedicated IR retainer with remote and on-site response times and minimum staffing hours defined by a Service Level Agreement (SLA) with each unit of the executive branch. This service will allow faster time to mitigation and response, while ensuring pre-arranged service-levels are understood and discussed prior to an incident.
- **Data Forensics:** Experienced forensic analysts use a combination of forensics tools and best practices to identity incident-related evidence, artifacts, and digital information across networks and devices, to perform root causes analysis, develop an incident timeline, maintain chain of custody, recommend containment and eradication procedures, recover damaged or lost files, and communicate to stakeholders. DoIT OSM should develop well-defined Data Forensics services provided to all Executive Branch units of Government.
- **Cyber Resiliency Planning:** DoIT OSM has previously worked with 3rd party experts in cyber resiliency to create Disaster Recovery Plan and Business Continuity Plan templates.
- **Tabletop Exercises**: DoIT OSM should offer Table Top Exercises at the Secretary-Level (Executive-Branch-Wide), Agency Executive Level (e.g. Secretary, Attorney General, CIO, CISO, and all other IT leaders), and Agency Operations Level (e.g. Infrastructure, Network, Platform, Application Development, and Security Teams). These tabletop exercises should be scoped for a specific group with defined outcomes and goals, such as improved communication between the legal department and the Maryland Department of Emergency Management.
- **Attack Emulation:** DoIT OSM should offer agencies the opportunity to engage with both Red Team and Blue Team professionals to conduct Purple Teaming Exercises using Breach and Attack Simulations (BAS) designed to emulate an adversary's behavior both inside and outside of a network. These engagements can provide immediate feedback on improvements that can be made to strengthen cybersecurity defenses.
- **Threat Hunting:** DoIT OSM should offer a defined periodic and continuous threat hunting service that provides detailed, exposure-related information concerning an immediate vulnerability and threat presenting risk to the State.

By offering these comprehensive incident response services, the Maryland Government's Executive Branch can leverage the expertise and resources of the DoIT OSM team, bolstering their incident response capabilities. This approach ensures a

proactive and unified response to cyber threats while centrally managing and coordinating resources for maximum efficiency and effectiveness.

4.3 Establishment of Centers of Excellence

In pursuit of centralized and effective management of the State's incident response program, DoIT OSM is currently developing Centers of Excellence. These CoEs are designed to offer comprehensive guidance, resources, and program materials aimed at enhancing the IT security program of each government unit. Scheduled for delivery in 2023, the initial CoE templates include:

- Incident Response CoE
- Cyber Risk Management CoE
- Business Continuity Planning CoE
- Disaster Recovery Planning CoE
- Disaster Recovery Business Services & System Inventory Template

Each CoE centers on empowering organizations with organization-specific documents and processes, overseen by their designated Information Security Officer (ISO). These resources enable detailed planning and preparation for potential cybersecurity incidents. For instance, the Cyber Risk CoE encompasses a planning phase involving the identification of critical business processes, data sources, and vendors. Subsequently, the unit of State Government can execute the Cyber Risk CoE by registering initial risks into a risk registry, including insights from previous risk assessment, vulnerability scan results, adversary emulation test findings, and cyber threat intelligence.

As the development of CoEs progresses, DoIT OSM remains committed to building comprehensive documentation, workbooks, and templates. These invaluable tools will be provided to Executive Branch units of State Government, fostering continual improvement of incident response processes.

4.4 Establishment of a Statewide Asset Inventory

Accurate and regularly updated asset inventories are foundational to the success of incident response, metrics reporting, and cyber resiliency initiatives outlined by the State Cybersecurity Centralization Plan. To ensure comprehensive asset tracking across all Executive Branch units of State Government, DoIT OSM recommends focusing on the following key asset categories:

1. **Users:** This includes employees, contingent workers, contractors, and service accounts.

2. **Business Services:** High-Level services supported by one or more systems, spanning on-premise and cloud-based hardware, network appliances, domains, IP addresses, etc.
3. **Systems:** (May be part of a business service; including designation as a High-Value Assets or HVA; May include designation as a Web Application)
4. Database Servers and Associated Databases.
5. **Endpoint Hardware Assets:** Workstations, laptops, tablets, mobile devices, etc.
6. **Network Hardware Assets:** Firewalls, switches, routers, hubs, gateways, proxy servers, web application firewalls, load balancers, etc.
7. **IoT Devices:** Printers, cameras, projectors, smart displays or TVs, etc.
8. **Web Applications and Websites:** Both public-facing and internal.
9. **Software as a Service (SaaS):** Applications on Hosted by 3rd Party Vendors
10. **Cloud Environment Assets:** Workloads, servers, IaaS/PaaS/SaaS applications, etc.
11. Software Assets
12. Interconnections between State Networks and External Networks

4.4.1 Centralization of Asset Inventories

The first vital step in protecting the state's information technology assets is having a clear understanding of what to protect. Accurate, regularly updated asset inventories are key to accomplishing the following goals outlined in the State Cybersecurity Centralization Plan:

- Ensuring the MDSOC is receiving all basic logs for all assets required to detect, investigate, respond-to, and remediate cybersecurity incidents.
- Properly inventorying, monitoring, patching, and protecting all high-value assets (HVAs), high-impact systems, and enterprise IT systems such as Active Directory.
- Establishing core metrics related to security improvements, IT & cyber accountability, and log collection success.
- Facilitating fast, cyber-resilient incident response by identifying business services and systems must be immediately restored following a major incident.

DoIT OSM recommends all Executive Branch units of State Government regularly collect, update, and provide asset inventory data to a centralized Configuration Management Database (CMDB).

4.4.2 Standardization of Asset Attributes

Standardization of Asset Attributes is equally important to ensure consistency and effectiveness in asset management. To achieve this, DoIT OSM should develop a common set of attributes for each tracked asset, such as owner, unit of government,

date purchased/issuance, etc. For complex business services, top-level documentation should include all dependencies, like databases, application servers, IP addresses and domain names with the associated dependencies mapped for each service.

4.4.3 Building a Centralized State Asset Inventory

DoIT OSM is taking the lead in creating a statewide asset inventory that brings together all Executive Branch assets into one database, regularly updated in almost real-time. This inventory will bridge the gap between different systems and reveal areas where coverage might be lacking, like workstations without specific applications, unmanaged mobile devices, or devices needing critical patches or operating system updates.

The plan is to have this system running by the end of 2023, allowing key stakeholders in Executive Branch units of government to easily access to their own asset inventories. This will enable continuous monitoring and help identify any gaps that need attention and improvement.

4.5 Providing Improved Training Opportunities for MDSOC Analysts

Effective incident response requires MDSOC team members to be well prepared in identifying, investigating, containing, eradicating, and recovering from cybersecurity incidents. Strong communication, analysis, and documentation skills are vital for incident triage to promptly assess whether an incident poses a significant threat to the State's network, systems, or data.

To ensure MDSOC Analysts are equipped with the necessary expertise, DoIT OSM offers a range of training opportunities:

- **MDSOC Analyst Onboarding Training:** This comprehensive training covers system, applications, equipment, and account reviews, emphasizing communication, scheduling, ticketing, and incident triage expectations. MDSOC Analysts are exposed to over 60 knowledge areas, including essential tools for incident investigation and analysis.
- **MDSOC Analyst SIEM Training:** This series of eLearning courses provide basic training on utilizing fields and visualizations in the state's SIEM solution. Advanced training is available through instructor-led sessions and credit-based classes.
- **MDSOC Analyst Endpoint Detection and Response (EDR) Training:** Available via the vendor's robust online training platform, MDSOC Analysts receive hands-on, virtual training using the state's EDR system for hands on detection, response, and remediation.

- **MDSOC Analyst Identity Threat Protection (ITP) Training:** Available via the vendor's robust "university system," MDSOC Analysts receive hands-on, virtual training use the state's Identity Threat Detection and Response (ITDR) system.
- **Advanced Incumbent Cybersecurity Training:** Available via instructor-led training for all approved State Employees, MDSOC Analysts working full-time for the State may participate in training covering all areas of the Certified Information Systems Security Professional (CISSP) and Security + certification exam.

Future activities conducted by DoIT OSM should ensure continued advancement of SOC Analyst skills and capabilities, including:

- **Attack Emulation Engagements:** The MDSOC Analysts should participate in annual purple-teaming activities that emulate cyber-attacks that may be faced by the State of Maryland. MDSOC Analysts would participate in these activities from a purple team perspective, performing defensive tasks alongside adversary emulation testers that will improve the analysts overall ability to protect State IT systems and data by teaching them tools, techniques, and procedures used by adversaries.
- **OSM Team Cross Training:** All analysts should have the ability to work alongside colleagues in a variety of cybersecurity roles, including GRC analysts, CTI analysts, vulnerability analysts, and cybersecurity engineering. Similar to the program provided for DoIT OSM interns, a rotation program should be developed to provide a deep, technical understanding of all team member roles to help broaden collaboration, foster respect, and improve incident response.

4.6 Mass Communication Capabilities

In the aftermath of a cybersecurity incident, the prompt and accurate dissemination of information to all impacted users within the Executive Branch units of State Government is of utmost importance. Recognizing this critical need, DoIT OSM is pursuing the procurement of a centralized mass communications platform equipped with pre-built templates for rapid dissemination of information. This platform will facilitate seamless communication between key stakeholders, including the Governor's Office, agency executive leadership, IT leadership, DoIT operations, and DoIT Office of Security Management.

Under the vigilant oversight of the Director of Cyber Resilience, the centralized mass communications platform will play a pivotal role in delivering critical incident response information to all users, be they employees, contractors, contingents, or other personnel. This coordinated effort ensures that pertinent updates and guidance reach every affected individual without delay.

5. Centralizing Log Collection & Monitoring

On August 27, 2021, the Executive Office of the President, Office of Management and Budget (OMB) released Memorandum 21-31 highlighting the significance of investigative and remediation improvements in cybersecurity incident response. The memorandum that the invaluable role of log sources from on-premise and cloud-hosted systems in detecting, investigating, and remediating cyber threats.[5] Building upon this guidance, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released a complementary document titled "Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities." This guidance outlines specific requirements for logging various event types based on an organization's maturity level and the prioritization of high-value assets (HVAs), high impact systems, and core enterprise IT systems such as Active Directory[6].

Considering this guidance, all Maryland State Executive Branch units of government should centralize logs in DoIT OSM's MDSOC. By consolidating logs in a centralized location, DoIT OSM can significantly enhance Maryland's cybersecurity incident visibility and response capabilities.

By adhering to OMB's Memorandum 21-31 and the subsequent CISA guidance, Maryland's Executive Branch units can proactively elevate their cybersecurity posture, ensuring a swift and coordinated response to potential incidents. The centralized log management under DoIT OSM's MDSOC will empower the State with actionable insights, facilitating timely incident detection, investigation, and remediation. This approach is essential in safeguarding critical assets and data, effectively mitigating risks, and fortifying Maryland's overall cybersecurity resilience.

5.1 Minimum Logging Requirements

The effective detection, investigation, containment, eradication, and response to cybersecurity incidents by the 24/7 MDSOC heavily relies on the logging of specific sources. These log types and events have been carefully prioritized based on CISA's

[5] Young, Shalanda. "Memorandum for the Heads of Executive Departments and Agencies" (official memorandum, Washington, DC: Office of Budget and Management, 2021) https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[6] CISA. "Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities" (Washington, DC: Department of Homeland Security, CISA, 2022) https://www.cisa.gov/sites/default/files/2023-02/TLPpercentage20CLEARpercentage20-percentage20Guidancepercentage20forpercentage20Implementingpercentage20M-21-31_Improvingpercentage20thepercentage20Federalpercentage20Governmentspercentage20Investigativepercentage20andpercentage20Remediationpercentage20Capabilities_.pdf

guidance[7] to ensure comprehensive coverage. The following log sources represent the basic, minimum logging requirements:

Log Type	Event Type
Identity and Access Management (IAM) Authentication Logs	• Changes in attributes and credentials, including create, update, delete. • Usage of credentials, such as successful and unsuccessful log-in attempts to all on-premise and cloud IdP sources (e.g. Okta, Azure AD, On-Prem AD, etc.)
Endpoint Logs (Servers, Workstations, Laptops)	• Process creation • Remote terminal or equivalent access and log off (success/failure) • System access and logoff (success/failure) • Scheduled task creation or changes • Service status changes (start, stop, fail, restart, etc.) • Active network communication with other hosts • Command-line interface (CLI) usage • PowerShell command execution • Windows Management Instrumentation (WMI) Events • Installation or removal of storage volumes or removable media • Linux Event Logs, including General System Activity, Authentication, Kernel Activity, Failed Logins, Mail Server
Network Logs	• Domain Name System (DNS) queries and response logs • Dynamic Host Configuration Protocol (DHCP) lease information including media access control (MAC) address and IP address. • Firewall logs (All edge firewall syslog) • Web Application Firewall (WAF) logs
Cloud Environment Logs	All activity with break glass accounts, which should never be used
Amazon Web Service Events	AWS CloudTrail
Microsoft Azure Cloud	Azure Active Directory Logs, Azure Activity
Microsoft 365 Logs	Unified audit log (with advanced features)

[7] Ibid.

Log Type	Event Type
Google Cloud Logs	Admin audit logs
Email Logs	Email logs including suspicious emails sent, received, or market as phishing, malicious attachments or links, unique forwarding rules, and impersonation or spoofing attempts

5.2 Advanced Logging Requirements

In the event of a cybersecurity incident, additional logging capabilities are required to effectively detect, respond to, and remediate a cybersecurity incident. The following log sources are highly recommended in addition to the Level 1 Logging Requirements, and have proven to be invaluable before, during, and after incident response:

Log Type	Event Type
Additional Network Logs	• Routers, switches, and wireless access points including 72 hours of PCAP logs. • Internal firewall logs set-up to air gap networks
Web Application Server	• Authentication attempts and other activity performed on a web server.
Mobile Device Logs	• UEM, MDM, RMM or other tool enrollment, de-enrollment, or detections
Secure Web Gateway or DNS Proxy	• IP, URL, or Domain Connections to malicious sites • Traffic to and from blocked or monitored 3rd party applications or sensitive content
Cyberthreat Intelligence (CTI)	• Indicators of Compromise (IoCs), Indicators of Attack (IoAs), and Artifacts
Privileged Access Management	• Administrator activities while using the Secret Server or Endpoint Privilege Management solution
Virtual Desktop Interface (VDI)	• VDI authentication, usage, and events for all VDI solutions

Log Type	Event Type
Data Loss Prevention (DLP) for Email, Cloud Drives, and Endpoints	• Use of sensitive or regulated data in emails, in documents, and on endpoints • Transfer of unstructured data files with sensitive or regulated data types between endpoints, media drives, and cloud drives
Cloud Access Security Broker (CASB)	• Successful and unsuccessful access to SaaS applications • User of SaaS applications, including events such as exporting of data and configuration changes

5.3 Logging Enrichment Data Requirements

To optimize incident investigation, triage and response, all Maryland State Executive Branch units of government are strongly advised to collect the following data into a centralized SIEM system. This data provides essential contextual information crucial for enriching the IR process and understanding the impact on users, systems, networks, and data.

Log Type	Event Type
Configuration Management Database (CMDB)	• Configuration Items, Business Services, CI/Service criticality, Dependencies, Patching Histories, Backup information, Business Owner, Technical Owner
Hardware & Endpoint Inventory	• HAM/UEM data, including ownership, assigned department, support group, date of issue, business use, and data/business criticality
Business Service, Application, and System Inventories	• Provide context around specific business service, application, or system ownership, support groups, departments, and other key data such as IPs, domains, URLs, SSO connections, and support staff
Software Inventory	• Provides context around software deployed to and managed by local IT staff, including potential out-of-date or end-of-life software, business use, criticality, etc.

Log Type	Event Type
Vulnerability Scan Reports	• Provides hardware, software, and OS vulnerabilities helpful in understanding what may be exploited during an incident or the effectiveness of patching processes

5.4 Implementation of MDSOC Detection Rules

Using Basic Logs collected by all Executive Branch Units of Government, detection rules should be established within a centralized SOC based on log source. Baseline detection rules for identities, networks, endpoints, email, and cloud environments must be established. The DoIT OSM MDSOC is currently building a core set of detection rules, alerts, and alerting logic, mapped to MITRE ATT&CK techniques and tactics, to add significant value to the SOC's capability to detect, respond to, and remediate incidents.

The following serve as examples of detection rules that should be established by the MDSOC using the basic logs provided by all Executive Branch units of Government:

Log Type	Example Detection Rules
IAM Authentication Logs	Repeat login sources and targets, privileged account login success and failures, privileged account or group creation or modification, excessive internal or external connections, anomalous or unusual logins or use of RDP, stale or inactive account logins, anomalous user behavior, compromised credentials, etc.
Operating System Logs	Access to or download of malware and potentially unwanted programs, Suspicious creation of processes, scheduled tasks, registry operations, PowerShell scripts, commands, or kernel drivers, specific exploit mitigation or prevention, ransomware Indicators of Compromise (IoCs), Indicators of Attack (IoAs) such as code injections or webshells, and lateral movement..
Network Logs	Deviations from baseline network traffic volumes, TCP resets and connection teardowns, suspicious user agent strings, malicious URL requests, web application firewall (WAF) suspicious or unusual patterns, high volumes of WAF HTTP status codes, WAF bypass attempts, rule changes, or data exfiltration

Log Type	Example Detection Rules
Cloud Logs	Data exfiltration form cloud sources, unsuccessful access attempts to cloud resources, non-admin resource creation and deletion, permission changes, unusual resource activity, configuration changes
Email Logs	Suspicious or malicious attachments uploaded, sent, or downloaded, mailbox rule changes, multiple user emails forwarded to same location, malicious links, quarantined emails

6. Defining Metrics & Reporting

To ensure transparent and effective budgetary appropriations and consistent performance evaluation across IT and cybersecurity teams, it is imperative for DoIT OSM to develop a comprehensive “Cybersecurity Metrics and Reporting Framework.” This framework should be designed to aggregate data from multiple platforms and present tailored dashboards to specific audiences, including:

- Governor’s Office and Cabinet Secretaries:
  - Dashboards providing a high-level overview of the state's cybersecurity posture, key performance indicators (KPIs), and critical incidents.
  - Metrics demonstrating the overall effectiveness of cybersecurity measures and their alignment with strategic objectives.
- DoIT Leadership (Secretary, Deputy Secretary, CISO, CTO):
  - Dashboards focused on strategic cybersecurity initiatives, risk management, and compliance.
  - Metrics showcasing the efficiency and impact of cybersecurity investments and efforts.
- Agency Leadership (Secretaries, CIOs/CISOs and Assistant Secretaries):
  - Tailored dashboards highlighting cybersecurity risks, incidents, and response capabilities within their respective agencies.
  - Metrics illustrating the effectiveness of security measures and resource utilization.
- Agency IT Managers:
  - Dashboards offering granular insights into specific IT and cybersecurity operational metrics and performance.
  - Metrics tracking key operational areas, such as incident response times, vulnerability management, and compliance.
- Individual IT or Security Teams:

- Customized dashboards providing team-specific metrics, enabling a focused understanding of their contributions to the broader cybersecurity program.
- Metrics evaluating the team's performance in areas like incident handling, security training, and adherence to policies.

By implementing a well-structured "Cybersecurity Metrics and Reporting Framework," DoIT OSM can foster accountability, transparency, and continuous improvement in the state's cybersecurity efforts. This data-driven approach will empower stakeholders at all levels to make informed decisions, optimize resource allocation, and strengthen Maryland's overall cybersecurity resilience.

6.1 Executive Metrics

Executive reports and dashboards should focus on the metrics that provide input on the overall health of the cybersecurity program from a budget, risk, and consumption standpoint. The following are suggested example metrics:

- Investments & Expenditures: Total DoIT Operational and Dedicated Purpose Account (DPA) Budget and Expenses by Category (Resources, Tools, etc.) by Fiscal Year
- Compliance Reporting: Total and percentage of Executive Branch Agencies Compliant with State Minimum Security Requirements by Control
- Cybersecurity Service Consumption: Total and percentage of agencies consuming DoIT OSM's Security Awareness Training
- Cyber Project Portfolio Health: Budget, scope, and schedule health for cyber projects. Total and percentage of endpoints with the state's EDR solution installed by agency
- State Risk Reporting: Total critical, high, medium, and low risks by agency
- Cybersecurity Operations: Total and percentage of incidents, threats, and vulnerabilities by criticality level by agency
- Control Health: Total and percentage of state systems meeting ATO requirements in the state's IT security manual

6.2 Cybersecurity Program Outcome-Driven Metrics

Cybersecurity program outcome-driven metrics (ODMs) should be developed to evaluate the efficacy and performance of the State's cybersecurity program. As the State continues to centralize cybersecurity, metric trends can indicate performance improvement. For example, DoIT OSM should track the Total and percentage of Agencies that submit complete asset inventories on a regular basis. An increase in this percentage over time would indicate improvement in data collection and exposure management. Conversely, DoIT OSM should track the Total and & of High Value

Assets (HVAs) with Critical or High Publicly Exploitable Vulnerabilities. A decrease in this percentage over time would indicate an improvement in patching.

For each Agency Leadership, Agency IT Managers, and Individual Teams, metrics, at a minimum, should focus the ODM categories and examples below:

Metric Category	Example Metrics
Asset Visibility & Coverage	Total and percentage of Agencies Submitting Complete and Accurate Asset Inventories to DoIT OSM
Logging Health	Total and percentage of Agencies Submitting Basic Level 1 Logs to DoIT OSM's Security Operations Center
Identity & Access Management	Total and percentage of Users with Compromised Passwords by Agency Total and percentage of Stale Users Not Authenticating for 90 Days by Agency
Vulnerability Management	Total and percentage of Assets Without Critical Patches after 30 Days of Release by Agency Total and percentage of Public-Facing Assets with Critical or High Vulnerabilities by Agency
Network Protection	Total and percentage of Firewalls Receiving MDSOC Indicators of Compromise and Cyber Threat Intelligence by Agency Total and percentage of Firewall Configurations Reviewed in Past Month
Endpoint Protection	Total and percentage of Servers with Advanced Endpoint Detection & Response
Mobile Device Protection	Total and percentage of Mobile Devices enrolled in centralized MDM/UEM solution
Governance, Risk, and Compliance	Total and percentage of Agencies Receiving Cybersecurity Maturity Assessments in Last 12 Months
3rd Party Risk	Total and percentage of SaaS Vendors Completing Security Review in Last 12 Months
Cloud Security	Total and percentage of Cloud Workloads with Cloud Workload Protection Platforms Installed

Metric Category	Example Metrics
	Total and percentage of SaaS Platforms with Centralized Single-Sign On Total and percentage of SaaS Platforms Monitored by a CASB Solution
Data Security	Total and percentage of File Shares with Advanced File Activity Logging Total and percentage of NAS/CIFs with Anti-ransomware File Extension FPolicies Enforced Total and percentage of Endpoints with DLP Enabled Total and percentage of Cloud Environments (Email, Drives) with DLP Enabled
Backup, Recovery, and Resilience	Total and percentage of Server VMs with Immutable Backups Total and percentage of Transactional Database Servers with Real-Time, Immutable Backups Total and percentage of NAS/CIFs with Immutable Backups Total and percentage of mission-critical systems with recovery from backups fully tested and validated Total and percentage of high-value, mission-critical systems with manual COOP/BCP plans established and tested
Security Awareness	Total and percentage of Employees and Contractors Completing Security Training by Campaign by Agency Total and percentage of Employees Reporting or Clicking on Simulated Phishing Tests
Application Development	Total and percentage of Custom Applications with Regular Code Scans Total and percentage of Custom Applications with Security Architecture Reviews

6.3 Incident Response Performance Metrics

To evaluate the overall performance of DoIT OSM's Security Operations Center (MDSOC), as well as the MDSOC's ability to handle cybersecurity incidents, specific metrics should be monitored in real-time to ensure Service Level Agreements between

agencies and DoIT OSM are consistently met and/or exceeded. The following metrics should be tracked internally by DoIT OSM:

Metric Category	Example Metrics
SIEM Availability	Total and percentage of Log Collectors Operational Total Service Interruptions Total Uptime of Individual Log Sources
Continuous SOC Monitoring	Total False Positive Incidents Reported Total False Positive Phishing Emails Reported Average Time to Detect, Act, Contain, and Respond to Incidents
Service Performance	Total and percentage of Security Incident Tickets by Severity by Category by Status Average Time to Respond to Security Incidents Average Time to Close Security Incident Tickets
Incident Monitoring	Total and percentage of Incidents by MITRE ATT&CK Tactic/Technique Total and percentage of Incidents by Severity Total and percentage of Incidents by Reporting Mechanism and Reporting Entity (State, Local, Public Utility, Other)
Threat Intelligence	Total and percentage of IoCs Blocked by Threat Feed Total and percentage of IoCs Ingested by Defense Layer (e.g. Network)

6.4 Metric Trend Measurement

As the State of Maryland progresses with the centralization of cybersecurity operations under the State Cybersecurity Centralization Strategy, tracking metrics over time becomes crucial for assessing the effectiveness of these initiatives. DoIT OSM recommends implementing a robust metrics tracking system that highlights trending increases or decreases as an indicator of improvement or regression. Several key metrics should be closely monitored:

1. **Average Time to Respond to Incident Tickets:** A decreasing trend in the average time to respond to incident tickets indicates an improved incident response capability and quicker resolution of security issues.

2. **MITRE ATT&CK Techniques Utilized:** An increasing trend in the number of MITRE ATT&CK techniques used by adversaries highlights the need for additional protective defenses and raises situational awareness of emerging threats.
3. **False Positives:** Increases in the number of false positives may indicate the need for specific alert tuning to reduce unnecessary noise and improve the accuracy of threat detection.
4. **Stale User Accounts:** A decreasing trend in the number of stale user accounts points to enhanced identity lifecycle management and a potential reduction in security risks associated with inactive accounts.
5. **Training and Awareness Effectiveness:** Tracking metrics related to security training and awareness initiatives can gauge the effectiveness of the workforce in identifying and mitigating security risks.
6. **Patching and Vulnerability Remediation:** Measuring the time taken to patch vulnerabilities and remediate identified issues helps assess the state's ability to maintain a secure IT environment.
7. **Incident Frequency and Severity:** Monitoring the frequency and severity of cybersecurity incidents provides insights into the state's overall cyber resilience and identifies areas needing improvement.

To ensure meaningful insights from the tracked metrics, the data should be regularly analyzed and shared with relevant stakeholders, including the MDSOC and DoIT OSM. Continuous monitoring and proactive response to changing trends will allow for prompt action to address emerging cybersecurity challenges and maintain a robust cybersecurity posture for the State of Maryland.

7. Augmenting IT & Cyber Staff

The "Cyber Performance and Capacity Assessment: Observations and Recommendations Report" prepared for the Governor's Office by Ernst and Young LLP (EY) on December 21, 2022, recommends staffing increases for the Office of Security Management to meet Senate Bill 812 requirements. Based on a population of approximately 50,000 end-users and 100,000 assets, the EY team noted that DoIT OSM is "considerably understaffed" to centralize cybersecurity efforts for the state. The recommendations note a required increase from 44 total employees in December 2022 (5 state employees, 39 contractors) to a total of 68-106 state employees plus contractor full-time equivalent (FTE) resources.

As of June 2023, after moving the Identity and Access Management team to DoIT OSM, the team currently consists of 69 total staff, including 19 state employees and 50 contractors. Staffing needs, which are subject to change, still exist as represented in the table below:

Office of Security Management Teams	Existing	State	Contractor	Needs
Executive Leadership and Management	7	6	1	1
Vulnerability Management	6	0	6	2
Cyberthreat Intelligence	5	0	5	1
MDSOC (Incident Response & Resilience)	17	2	15	3
Network Security	7	0	7	1
Governance Risk and Compliance	1	0	1	8
Data Security	0	0	0	4
Local Cybersecurity Program	1	1	0	1

Office of Security Management Teams	Existing	State	Contractor	Needs
Identity and Access Management	13	9	4	0
Enterprise Services and Project Mgmt.	7	1	6	2
Platform Engineering & Administration	5	0	5	1
Endpoint and Mobile Engineering	0	0	0	1
Total	**69**	**19**	**50**	**25**
Staffing Goals for FY 2024 & FY 2025	**94**	**40**	**54**	-

To ensure continued success of the State Cybersecurity Centralization Strategy and to bolster DoIT OSM, it is imperative for the State to allocate sufficient budget for growth. In parallel, DoIT OSM should remain committed to identifying, interviewing, and hiring skilled state employees who can drive the centralization effort forward. Additionally, augmenting existing staff with highly technical contractors capable of executing critical tasks required for cyber assessments, perform highly-technical services, and the centralization of technology, tools, logs, services, and incident response capabilities.

8. Increasing Cyber Service Offerings

DoIT OSM remains committed to the ongoing development of a centralized and comprehensive portfolio of cybersecurity platforms, technologies, services, and capabilities. To centralize purchasing and maximize return on investment, DoIT OSM recommends the State continue funding services purchased for all Executive Branch units of Government, adopting a similar model used to centralize Endpoint Detection and Response for the State. Standardization and centralization of these services not only optimizes investments in monitoring, detection, and logging technologies, but also streamlines incident response processes and procedures, leading to a more resilient and effective cybersecurity framework for the State. The following services are currently either fully implemented or should be implemented by DoIT OSM:

- **Endpoint Detection and Response (EDR):** The centralization of EDR services has already proven successful in enhancing the State's ability to detect and respond to potential threats on endpoint devices. This centralized approach ensures uniformity and efficiency in incident response across all Executive Branch units.
- **Network Detection and Response (NDR):** Managed Next-Generation Firewalls for Intrusion Prevention Systems (NGIPS) with annual control attestation to ensure compliance with state standards. Additional services include NetFlow analysis, threat intelligence integration, and additional IDS/IPS capabilities.
- **Security Information and Event Management (SIEM):** A centralized SIEM solution provides real-time monitoring and analysis of security events, enabling prompt detection and response to potential security incidents.
- **Threat Intelligence Sharing Platform:** Implementing a unified threat intelligence sharing platform enables the exchange of critical threat data and insights, empowering the State to proactively defend against emerging threats.
- **Incident Response Management Platform:** A centralized incident response management platform that streamlines incident reporting, tracking, and resolution, ensuring a consistent and coordinated response to cybersecurity incidents.
- **Vulnerability & Attack Surface Management Solution:** The centralization of vulnerability and attack surface management allows for a systematic approach to identify and remediate potential exposure and security weaknesses across the State's internal and public-facing IT infrastructure.
- **Security Awareness Training:** A standardized security awareness training program ensures that all personnel within the Executive Branch are educated on cybersecurity best practices, reducing the likelihood of human-related security incidents.

- **Identity and Access Management (IAM):** A centralized IAM solution helps to manage and secure user identities, access privileges, and authentication processes effectively.
- **Identity Threat Detection and Response (ITDR):** By leveraging authentication telemetry across on-premise IAM solutions and cloud-based IDaaS providers, ITDR solutions detect anomalous or malicious login behavior and identity-based threats.
- **Privileged Access Management (PAM):** Combined with IAM, PAM improves the security of privileged users, including the management of local administrators using a Privilege Elevation and Delegation Management (PEDM) solution.
- **Encryption and Data Protection Services:** Centralized encryption and data protection services safeguard sensitive information and ensure compliance with data privacy regulations.
- **Cybersecurity Incident Response Playbooks:** Standardized incident response playbooks guide the response team through predefined steps and procedures, enhancing incident resolution efficiency.
- **Continuous Monitoring and Auditing Tools:** Centralized continuous monitoring and auditing tools provide real-time visibility into the State's IT environment, enabling proactive identification of potential security threats.
- **Data Security:** By combining data discovery tools, including data classification and categorization capabilities, with data loss prevention (DLP) capabilities and services, sensitive data stored in files and databases can be better protected from destruction, misuse, exfiltration, or loss.
- **Secure Service Edge (SSE) Platform:** As the traditional network expands from on-premise to the remote locations, VPN solutions are no longer enough to protect the remote worker. SSE solutions protect web browsing, access to cloud platforms, access to on-premise networks, and data usage using a combination of CASB, ZTNA, DLP, and SWG solutions.

9. Conclusion

Maryland's State Cybersecurity Centralization Strategy encompasses crucial initiatives focused on enhancing incident response, fortifying log collection and monitoring, strengthening security metrics and reporting, increasing service offerings, and augmenting the cybersecurity and IT workforce. These efforts share a common objective: centralizing cybersecurity operations and incident response for Maryland's Executive Branch. Achieving this centralization necessitates the active collaboration and participation of agency leadership and IT executives. As adversaries continue to collaborate and utilize advanced tools and capabilities to breach networks across U.S. networks, causing a potential total loss of $10.2 billion in 2022[8], the State must act swiftly to consolidate its efforts and collectively defend shared IT and data assets, ultimately benefiting all Maryland constituents.

The 2023 State Cybersecurity Centralization Strategy serves as a comprehensive roadmap for advancing service capabilities in monitoring, logging, detection, and incident response. Its primary aim is to ensure that all units of State Government are well-prepared, adequately resourced, and equipped to safeguard against cyber-attacks effectively. This strategy acknowledges the evolving threat landscape and seeks to establish a robust cybersecurity framework capable of detecting, containing, eradicating, and recovering from potential cyber incidents.

The collaborative approach of agency leadership and IT executives, combined with these strategic initiatives, paves the way for a unified and resilient cybersecurity ecosystem. As Maryland continues its journey towards centralized cybersecurity operations, it strengthens its ability to protect critical assets and data, ensuring the safety and security of its citizens and constituents in an increasingly interconnected and digital world.

[8] FBI Internet Crime Compliant Center. "Federal Bureau of Investigation Internet Crime Report" (Washington, D.C. 2022) https://www.ic3.gov/media/PDF/AnnualReport/2022_IC3Report.pdf