Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

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

SERVICE AGREEMENT

Between

The Maryland Department of Information Technology and

The Customer

for

Information Security Officer (ISO) Program – Advisory & Compliance Services

This Service Agreement between the Department of Information Technology and Customer is subject to the Memorandum of Understanding for Provision of Information Technology Services between the Maryland Department of Information Technology ("DoIT") and the Customer. The parties agree as follows:

I. Service Description

The Information Security Officer (ISO) Program (the "Program" or "Service") is a shared service provided by the Maryland Department of Information Technology (DoIT) to support State agencies in strengthening their cybersecurity posture. The Program is a key component of OSM's strategy to provide unified cybersecurity leadership, enhance statewide resilience, and foster a culture of security risk management across Maryland State government. The Program provides dedicated security expertise, guidance, and resources to assist agencies in meeting State and federal cybersecurity compliance requirements. The Service ensures that agencies have access to experienced cybersecurity professionals who can manage risks, implement security controls, and coordinate incident response efforts.

A. <u>Standard Service:</u>

The following components are included with the standard service:

1. Assignment of an ISO to support the agency, based on tier classification (see Section IV)
2. Evaluation of security risk assessments and recommendations for risk remediation

3. Policy and procedure development specific to the agency aligned with State security frameworks
4. Compliance support for state and federal regulations
5. Incident response coordination and reporting
6. Vendor risk management assistance
7. Security consultation and advisory services

B. Service Exclusions:

While the ISO Program provides critical cybersecurity expertise and advisory support, the following services are excluded from its scope:

1. Direct IT Operations Management – ISOs do not perform day-to-day IT security operations or manage IT infrastructure.
2. Development or Management of Customer Applications – ISOs do not design, develop, or maintain customer-specific applications.
3. Technical Support for Third-Party Technologies – ISOs do not provide maintenance, troubleshooting, or repair services for non-State-managed third-party tools, software, or services.
4. Full-Scale Incident Response and Forensic Investigations – ISOs support incident response coordination but do not conduct full forensic investigations or hands-on remediation; however, this capability may be covered by other State services.
5. Project Management for Customer Initiatives – ISOs do not serve as project managers for agency-specific IT or security projects.
6. Security Tool Implementation and Administration – ISOs provide advisory services but do not directly deploy or manage security tools on behalf of agencies; however, managed cyber services provided by the State may include this capability outside of the ISO program.
7. Physical Security Management – The Program does not cover physical security controls, such as badge access, or facility security operations.
8. End-User IT Support – ISOs do not provide help desk or IT troubleshooting services to end users.
9. Agency Responsibilities – ISOs do not replace roles, authorities, and decision making ability of agency stakeholders.

Agencies requiring services outside of the ISO Program's scope should coordinate with DoIT to determine if the Office of Security Management can fulfill their specific needs.

II. Service Dependencies

To ensure the Service is delivered consistently and in accordance with State standards, the Customer must satisfy the following requirements:

Technical:	● Provide access to agency security-related documentation and systems as needed
Non-Technical:	● Provide a minimum of two (2) 24 x 7 x 365 points of contact for coordinating outages, emergency maintenance/restoration, and change management ● Provide a minimum of one (1) primary point of contact for agency relations and ISO integration. ● Agency IT staff cooperation with meeting and working with their assigned ISO. ● Timely responses to all ISO outreach to include security findings and remediation efforts.

III. Program Responsibility to the Customer

The following is a non-exhaustive list outlining the responsibilities of both the ISO and the Customer. This list may be updated periodically, with any changes taking effect 14 calendar days from the posting date of the revised service agreement.

A. DoIT Responsibilities to the Customer

1. Assigning and managing qualified Information Security Officers (ISOs) appropriate to agency needs, informed by the service tiering structure outlined in Section IV.

2. Providing strategic cybersecurity guidance, consultation, and advisory services aligned with State goals, risk management principles, and industry best practices.

3. Conducting or facilitating security assessments and risk analyses (such as NIST CSF maturity assessments) to identify vulnerabilities, gauge security posture, and inform risk treatment and remediation efforts.

4. Developing and disseminating applicable State cybersecurity policies, standards, frameworks, and recommended best practices to guide agency security programs.

5. Coordinating Statewide cybersecurity initiatives, compliance tracking efforts (related to State and relevant federal requirements), and security-related communications relevant to participating agencies.

6. Assisting agencies in understanding and integrating with available centralized DoIT cybersecurity services to enhance security posture and achieve efficiencies.

B. Customer Responsibilities

1. Satisfy all requirements outlined in Section II, "Service Dependencies," including providing points of contact, necessary access, staff cooperation, and timely responses.
2. Actively manage and implement security remediations for identified vulnerabilities and assessment findings, aligning efforts with State cybersecurity requirements and risk priorities established in coordination with the ISO and agency leadership.
3. Ensure agency personnel, processes, and systems comply with applicable State security policies, standards, and frameworks disseminated by DoIT.
4. Cooperate fully with the assigned ISO, participate in security assessments and audits, and provide accurate information regarding agency systems, processes, and security controls.
5. Report security incidents promptly according to DoIT protocols and actively participate in incident response and coordination efforts as guided by the ISO and State incident response plans.
6. Retain ultimate authority and decision-making responsibility for the agency's operations, requests for risk acceptance, resource allocation, and implementation of security controls. The ISO provides advisory services, but the agency owns its security posture.

IV. Service Level Agreements (SLA’s)

All services provided under the ISO Program will be measured against the following Key Performance Indicators (KPIs):

Service Area	**Performance Standard**	**Measurement & Compliance**
Security Risk Assessments	Establish a baseline of the agency’s security posture within 12 business weeks of onboarding (or subsequent completion of assessment), using available assessment data, interviews, and existing	90% completion within timeframe.

	documentation to identify key risks and capability gaps.	
Risk Remediation Planning	Assist agency with developing a remediation plan within 8 business weeks of the agency's receipt and review of cybersecurity maturity assessment reports.	80% on-time delivery.
Incident Response Support	Respond to security incidents in accordance with established Statewide incident response policies.	100% adherence to response times.
Agency Requests	Respond to non-emergency agency cybersecurity requests within 2 business days.	90% on-time completion.
Compliance Support	Provide regulatory guidance and assessment within 10 business days of request.	85% on-time delivery.

ISO Program Support Tiering

The Information Security Officer (ISO) Program categorizes agencies based on their agency funded cybersecurity staffing and capabilities and the level of support required from the Office of Security Management (OSM). Agencies are assigned to Tier 1, Tier 2, or Tier 3, with Tier 3 agencies receiving the highest level of support due to significant lack of internal resourcing dedicated to cybersecurity.

This tiering system ensures that security resources are allocated effectively, prioritizing agencies that require the most dedicated efforts to enhance their security posture and mitigate risks.

Tier Level	Description	Service Expectations
Tier 1	Agencies with dedicated cybersecurity staff and a robust agency security structure	Periodic (monthly) ISO support, compliance assistance, and strategic guidance to align with State standards and services
Tier 2	Agencies with dedicated cybersecurity resources that have other job functions outside of cybersecurity	Moderate (bi-monthly) ISO support, increased remediation efforts, security assessments and dedicated assistance deploying centralized cyber services
Tier 3	Agencies with no dedicated cybersecurity resources or agency cybersecurity structure.	Frequent (weekly) ISO support, comprehensive remediation services, and ongoing security monitoring and focused deployment and prioritization of cyber service adoption

ISO Prioritization

- Tier 3 agencies receive the highest level of support due to their lack of dedicated support and funding within their agency for cybersecurity.
- OSM assigned Project Managers (PMs) in coordination with the agency, and the ISO leadership team assess agency maturity and align them with the appropriate tier to ensure tailored service delivery.
- Tier 1 and Tier 2 agencies receive structured support based on available resources, with a focus on compliance, best practices, and centralized cyber service adoption.

V. Support and Service Management

A. Support

- ISOs are available during standard business hours (8 hours a day, 5 days a week) to provide security guidance, assessments, and compliance support.
- ISOs may work beyond standard hours for critical incident response situations, ensuring that agencies receive necessary support during emergencies.
- Agencies will have access to 24x7 support via the Service Desk / Security Operations Center for security-related issues.

DoIT will provide support via telephone, email, or in-person according to the SLA’s outlined above.

The DoIT Service Desk is available 24 hours a day, 7 days a week to provide frontline telephone support.

Advanced support for more complex issues are available Monday through Friday, excluding State holidays and closings.

Specialized or expert-level support will be engaged as needed to address critical or escalated issues.

DoIT will serve as the primary support provider of the Service, utilizing third-party vendors as and when necessary.

While DoIT strives to tailor support and maintenance activities to align with the Customer's mission, certain limitations may prevent us from fully accommodating evolving business needs. As such, support and service management activities under the ISO Program do not include provisions noted in section I.B.

VI. Costs for Service

This service is provided at no cost to State executive branch agencies and entities. DoIT provides this Service via a shared service model, which allows the State to recognize reduced costs based on economies of scale achieved through centralization of program support.