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

Web Application Scanning (WAS)

This Service Agreement forms a part of the Memorandum of Understanding between the Maryland Department of Information Technology ("DoIT") and the Serviced Customer. The parties agree as follows:

I. Service Description

The Web Application Scanning service is a DoIT Office of Security Management (OSM) security service offering vulnerability scanning of Customer external web applications as well as prioritization and tracking of the remediation activities. This service is supported by a dedicated team that manages the customer onboarding process, configures and schedules the customer's scan policies, provides vulnerability reporting, maintains the vulnerability management platform, and troubleshoots platform issues that may arise.

The service includes the following features and components:

A. Standard Service:
The following components are included with the standard service:
1. External vulnerability scanning of most modern web applications
2. Platform administration and support
3. License management
4. Vulnerability reporting

B. Service Exclusions:
The following elements are excluded from the standard service offering:
1. Agent-based vulnerability scans
2. Network-based vulnerability scans
3. Discovery scans
4. Vulnerability remediation
5. Web application penetration testing

C. Optional Services
1. At this time there are no optional services offered in this area by DoIT

II. Service Dependencies

To ensure the service described herein is delivered consistently and in accordance with state standards, the customer must meet the following requirements:

DoIT Services:	• User's must have accounts in the statewide directory (@maryland.gov) email system in order to gain access to the platform • Configure the customer Tenable Web Application Scans • DoIT Service Desk • Maryland Security Operations Center (MDSOC)
Technical:	• **Network Connectivity:** Web applications must be publically accessible in order for the cloud based scanners to perform the scans.
Non-Technical:	• **Point of Contact**: The Customer must provide a point of contact for troubleshooting Web Application Scans and remediating open vulnerabilities • **Web Application Scanning (WAS) requirement(s)**: Customers must provide the list of fully qualified domain names (FQDNs) for web application scanning • **Data Requirement(s):** Customers must provide their list of critical applications, critical servers, and public facing application URLs.

III. Responsibility Model

The following contains a non-exhaustive list that describes the responsibilities for both DoIT and the customer and may be updated periodically. Updates will be considered effective 14 calendar days from the posting date of the new service agreement.

A. DoIT Responsibilities for Customer
DoIT shall be responsible for the following activities in coordination with the Customer receiving DoIT enterprise managed Web Application Scanning Vulnerability Management services:

1. Provide full administration of the Tenable vulnerability management platform
2. Troubleshoot Tenable platform and web application scanner misconfigurations
3. Provide vendor contract management

4. Maintain Tenable licenses and monitor usage
5. Investigate and address false positive vulnerabilities
6. Serve as the escalation point for Tenable platform issues
7. Provide vulnerability management support: M-F, 8AM - 5PM
8. Retain customer vulnerability data for 90 days
9. Configure scan policies, scan schedules, and customer access
10. Provide remediation prioritization guidance

B. Customer Responsibilities

The Customer shall be responsible for the following activities:

1. The Customer must provide a point of contact for troubleshooting web application scan misconfigurations and issues.
2. The Customer is responsible for submitting a DoIT Service Desk ticket to request access to the Tenable vulnerability management platform (Non-Enterprise customers only).
3. The Customer is responsible for opening support tickets with the DoIT Service Desk to request support from DoIT.
4. The Customer is responsible for reporting security issues to the Maryland Security Operations Center (MDSOC).
5. The Customer is responsible for providing the list of fully qualified domain names (FQDNs) that need to be scanned for vulnerabilities and keeping it updated via DoIT Service Desk support tickets.
6. The Customer is responsible for providing the list of critical applications, critical servers, and public facing application URLs.
7. The Customer is responsible for remediating Critical severity vulnerabilities within 15 calendar days, High severity vulnerabilities within 30 calendar days, Medium severity vulnerabilities within 60 calendar days, and Low severity vulnerabilities within 90 calendar days.
8. The Customer is responsible for staying in compliance with their licensing agreement and paying for additional licenses when needed.

IV. Service Level Agreements (SLA's)

A. Availability

Service availability includes the duration of time the service is operational during a calendar year and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	Web Application Scanning platform availability target is 99.9% for 24x7x365 operations ● DoIT OSM Web Application Scanning support: M-F, 8AM - 5PM, excluding state approved holidays ● MDSOC incident support: 24x7x365

B. Maintenance
DoIT may modify the service without degrading its functionality or security features.

1. Scheduled Maintenance
Regular maintenance must be performed to maintain availability and reliability standards and includes replacing hardware, upgrading software, applying patches, and implementing bug fixes.
    a) Scheduled maintenance will be performed outside of normal business hours (7 pm - 6 am Monday - Friday; weekends and holidays)
    b) The customer will be notified no less than five (5) business days prior to the scheduled activity.
    c) Within twenty-four (24) hours after the completion of the scheduled activity, the Customer will be notified.

2. Unplanned Maintenance
    a) DoIT will attempt to notify the Customer of any unplanned maintenance activities no less than two (2) hours prior to commencement. Note: Emergency activities requiring immediate remediation may not allow ample time for notification.
    b) Within twenty-four (24) hours after the completion of unplanned maintenance activity, the Customer will be notified.

C. Service Delivery
DoIT will deliver the requested services to the customer in a timely manner according to the following standards.

Category	Measure
Normal Changes	Normal changes will be assigned to a vulnerability analyst within 1 business day of being assigned to the Vulnerability Analyst Service Now assignment group
Emergency Changes	Emergency changes will be assigned to a vulnerability analyst immediately after being assigned to the Vulnerability Analyst

	Service Now assignment group

V. Support and Service Management

A. Support

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

1. The DoIT Service Desk is available twenty-four (24) hours a day, seven (7) days a week, to provide Tier 1 telephone support.
2. Tier 2 support will be provided during regular business hours (8 am - 5 pm) Monday thru Friday, excluding state holidays and state closings.
3. Tier 3 support will be provided as needed to address further escalations
4. DoIT will serve as the primary support provider of the service outlined herein except when third-party vendors are employed.

B. Incident Management

Incidents reported to the DoIT Service Desk will be triaged and managed based on priority as follows*:

Priority (P)	Description	Response Time	Resolution
Priority 1:Critical Impact 1: Critical Urgency 1: High	An incident that results in a total cessation of service across the Customer. Involves the loss of a critical business service or function ● The impact is statewide or affecting a public facing/revenue generating service on a widespread level. ● Multiple public safety and critical citizen systems/applications are impacted ● The disruption could result in regulatory, security, or reputational impact	2 Hours	24 hours
Priority 2: High Impact 2: High Urgency 1: High	An incident that results in a partial cessation or disruption of service, administrative access issues, or loss of other essential business functions. An issue is affecting a business component that isn't critical but is resulting in a disruption of the business service. Users are unable to	4 hours	2 business days

	perform normal business operations, and a workaround is not available. ● The issue can impact multiple agencies or a subset of multiple users ● The issue is affecting a high-level Executive.		
Priority 3: Moderate Impact 3: Normal Urgency 1: High	Disruption of service for non-essential functionality, service questions, and administrative requests such as account creation, deletion, and changes. The impact causes a work stoppage for a single user - a work around is not available ● A single user is not able to complete a time sensitive critical task ● The user is marked as a VIP	2 business days	5 business days
Priority 4: Normal Impact 3: Normal Urgency 2: Medium	Minimal impact on business operations and can be resolved without significant disruption. A minor cosmetic issue on a non-critical webpage could be an example. ● An incident has impaired the user's ability to perform their normal business operations but a work around is available ● An issue is affecting a single user that is not business critical or time sensitive	4 business days	7 business days

C. Request Management
Requests to move, add, or change service shall be handled as follows:

New Service(s)

Entities seeking to utilize the service or deploy optional services outlined herein must:

a) Submit a request via email to doit.intake@maryland.gov explaining the business needs or challenges.
   (1) DoIT will evaluate the request to ensure that the service meets the entity's business needs.

Service Modifications

To increase, decrease, or alter existing service, the Customer must:

a) Submit a request via email to doit.intake@maryland.gov
   (1) Service modifications include increasing or decreasing the quantity of WAS targets. DoIT will log the request and assign it to the appropriate team for fulfillment.
   (2) Requests that involve increases to costs will result in billing changes to the agencies which will require a Statement of Work and fund certification to make the change.

D. Outages
DoIT will notify the Customer via email of any outages or service degradation resulting from maintenance, fault isolation, or other disruptions.

E. Support and Service Management Exclusions:
While DoIT strives to tailor support and maintenance activities to match the customer's mission, there may be limitations that hinder our ability to satisfy changing business needs. As such, support and service management activities do not include:

Development or management of customer applications
Repairs or services for the customer's third-party technologies.
Spearheading Customer initiatives
Project management

VI. Costs for Service

DoIT provides this service via a shared service model, which allows the state to recognize reduced pricing based on economies of scale.

A. All services delivered by DoIT under this agreement will be supported via OSM appropriated funds unless identified consumption or specific requirements demand additional costs to support.

VII. Termination of Service

This service will automatically be renewed unless the customer and DoIT mutually agree in writing to adjust or discontinue.

A. Due to the nature of the managed service and its alignment to the Statewide Cybersecurity Centralization Strategy, termination requires written authorization by the State Chief Information Security Officer (CISO). If approved, terminations will only be effective at the end of the fiscal year.

VIII. Warranty, Limitations, and Exclusions

A. N/A