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

Vulnerability Management (VUL)

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 Managed Vulnerability Management service is a DoIT Office of Security Management (OSM) security service offering scanning capabilities as well as prioritization and tracking of remediation activities across internal and external network devices, servers, workstations, web applications, and other assets on-premises and in cloud environments using agent-based, compliance, and external network scans. 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 any 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. **Agent-Based Scanning**: Automated, vulnerability scanning that uses a locally installed program (agent) to scan the local host to identify potential weaknesses.
2. **Compliance Scanning**: Automated, policy compliance audits of supported systems.
3. **External Network Scanning**: Automated, vulnerability scanning that scans your external-facing systems to identify potential weaknesses.
4. Vulnerability Reporting
5. DoIT OSM support team
6. Vendor support

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Network-based scans
2. Discovery scans
3. Vulnerability remediation
4. Tenable Nessus Agent deployment to non-managed agencies
5. Custom compliance audits
6. Web application scans

C. Optional Services

1. N/A

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 account in order to gain access to the platform • Configure the customer Tenable tenant, Nessus Agent, and user account • DoIT Service Desk • Maryland Security Operations Center (MDSOC)
Technical:	• **System Compatibility:** Customer hosts must be compatible with supported Nessus Agent operating systems (Nessus Agents currently support Windows, Mac and many flavors of Linux) • **Network Connectivity:** Tenable Nessus Agents must have connectivity to Tenable.io over TCP port 443 • **Credentials**: Administrator credentials are required to install the Nessus Agent • **Agent Installation:** The Customer is responsible for installing the Nessus Agent on compatible hosts. DoIT performs this function for fully managed agencies
Non-Technical:	• **Point of Contact**: Customer must provide a point of contact for troubleshooting Nessus agents and addressing open vulnerabilities • **Data Requirement(s):** Customer must provide their list of critical applications, critical servers, and public facing application URLs

	• **Training**: Customer must understand how to deploy and link the agent to Tenable.io

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 Vulnerability Management services:

1. Provide full administration of the Tenable vulnerability management platform
2. Monitor Nessus Agent deployments to customer assets
3. Vendor contract management
4. Maintain Tenable licenses and monitor usage
5. Troubleshoot Tenable platform and Nessus agent issues
6. Investigate False Positive vulnerabilities
7. Serve as the escalation point for Tenable platform issues
8. Vulnerability Management support: M-F, 8AM - 5PM
9. Ensure 90-Day data retention
10. Customer Vulnerability Management configuration
11. Configure Customer tenant in the Tenable vulnerability management platform
12. Configure scan policies, scan schedules, Nessus Agent updates, and Customer access
13. Generate custom Nessus Agent linking string
14. Provide remediation prioritization
15. Execute agent-based vulnerability scans in support of Customer audits (Custom compliance scans are not supported)

B. Customer Responsibilities

The Customer shall be responsible for the following activities:

1. The Customer must provide a point of contact for troubleshooting Nessus agents
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 configuring network connectivity from assets with the Nessus Agent to the Tenable vulnerability management platform
4. The Customer is responsible for opening support tickets with the DoIT Service Desk to request support from DoIT
5. The Customer is responsible for reporting security issues to the Maryland Security Operations Center (MDSOC)
6. **Data Requirement(s):** The Customer is responsible for providing their list of critical applications, critical servers, and public facing application URLs.
7. **Patching:** The Customer is responsible for the remediation of third-party vulnerabilities and misconfiguration in compliance with the State of Maryland SLAs
8. **Vulnerability Remediation SLA:** 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
9. **Nessus Agent:** The Customer is responsible for installing the Nessus Agent on their covered assets (Non-managedCustomers Only)
10. **License Compliance:** The Customer is responsible for staying in compliance of their licensing agreement and paying for additional licenses needed when overages occur

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	Vulnerability management platform availability target is 99.95% production uptime

	• DoIT OSM Vulnerability Management support: M-F, 8AM - 5PM, excluding State approved holidays • MDSOC incident support: 24x7x365
Capacity	Vulnerability data is stored for 90 days in Customer data repositories
Reliability	Automatic appliance and plugin updates occur daily and may cause the user interface of the vulnerability management platform to be temporarily unavailable

B. Maintenance

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

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)

Unplanned Maintenance

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 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.	4 hours	2 business days

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
*Note: At times, it may be necessary to contact a vendor for assistance, thereby lengthening response times.			

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:

b) Submit a request via email to doit.intake@maryland.gov

(1) Service modifications include increasing or decreasing quantity of units, relocation of service.

(2) DoIT will log the request and assign it to the appropriate team for fulfillment.

(3) 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
Network-based scans
Discovery scans
Vulnerability remediation
Tenable Nessus Agent deployment (Non-Enterprise Customers)
Custom compliance audits are unsupported
Web application scans

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