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

User Entity

for

Cybersecurity Assessments and Penetration Testing

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

This service can consist of either a cybersecurity maturity assessment or a internal/external penetration test or a combination of both.The maturity assessment provides a high level analysis of current practices and gaps while the penetration test identifies weaknesses in application and organizational boundaries for unauthorized access mechanisms, and visibility into the issues with configurations and system lifecycle.

1. Organizational Security Maturity Assessment

- This component of the assessment will focus on organizational compliance with the security controls described in the IT Security Manual, structured using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the standards described in the Maryland IT Security Manual.

2. Web Application Scans and Penetration Test

- Internal Penetration Testing focusing on testing attacks that could be carried out by an adversary who has already gained a foothold within an enterprise network and seeks to elevate privileges, maintain persistence, and move laterally. Internal Penetration Tests shall be conducted on-site and under the supervision of the unit's security team to ensure proper detection and response mechanisms are in place.
- External Penetration Testing- The scope includes the evaluation of publicly accessible web applications, including both websites and APIs, and a remote organizational penetration test to identify potential weaknesses in organizational boundaries. Tests should be conducted using automated tools and manual tests.

A. Standard Service:

The following components are included with the standard service:

1. A Statement of Work (SOW) per engagement.
2. Security Maturity Assessment Report for the Maturity Assessment engagements.
3. Rules of Engagement document and Penetration Testing Report for Penetration Testing engagements.

B. Service Exclusions:

The following elements are excluded from the standard service offering:

1. Specific Remediation Activities.
2. All other exclusions will be per SOW.

C. Optional Services

Any optional services will be executed via the SOW.

The following services are add-ons that may be requested. Costs for these items are variable and will be clearly defined and agreed to before moving forward with the request.

1. Additional IP addresses and/or web applications for penetration testing

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:	• DoIT service dependencies to be identified following the engagement.
Technical:	• Provide POC(s) for pen testing in case of any issues, concerns, or critical vulnerabilities identified. • Access to systems/applications as applicable.
Non-Technical:	• Provide respective POC(s) for coordination and approvals.

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 User Entity
DoIT shall be responsible for the following activities in coordination with the User Entity receiving DoIT enterprise managed services:

1. Developing the SOW for and overseeing the engagement
2. Assigning a Point of Contact (POC) from DoIT
3. Executing vendor agreements
4. Notify the Security Operations Center (SOC) of the testing schedule when applicable

B. User Entity Responsibilities
The User Entity shall be responsible for the following activities:

1. Executing the SOW
2. Participation, as required, for the engagement
3. Providing payment for services
4. Complying with the terms outlined in the SOW
5. Providing acceptance of final report
6. Allowing access and permissions necessary to perform the functions/tasks.

IV. Service Level Agreements (SLA's)

A. Availability
Service availability includes the duration of time the service is operational during the period identified in the SOW and the level at which the service functions. The table below further outlines DoIT's service targets.

Category	Measure
Availability	Not Applicable
Capacity	Not Applicable
Reliability	Not Applicable

B. Maintenance
Not Applicable. All assessments and testing schedules will be determined via SOW.

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

Category	Measure

Initial Ticket Response and Customer Contact	Within five business days
Statement of Work	Within 14 business days
Draft/Final Reports	According to timelines established in the SOW

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. Request Management

Requests to move, add, or change service shall be handled as follows:

1. 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.
      - DoIT will evaluate the request to ensure that the service meets the entity's business needs.

2. Service Modifications
   To increase, decrease, or alter existing service, the User Entity must:
   a) Submit a request via email to doit.intake@maryland.gov
      - Service modifications include increasing or decreasing quantity of units, relocation of service, or scope of assessment or test.
      - DoIT will log the request and assign it to the appropriate team for fulfillment.
      - Requests that involve increases to costs will result in billing changes to the agencies which will require a modification

to the Statement of Work and fund certification to make the change.

b) Any other respective documentation to be modified [(ie. rules of engagement (ROE)] will be updated and required approvals processed.

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

D. 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, any support and service management activities that are not included are outlined in the SOW.

VI. Costs for Service

DoIT provides this service via costs outlined in an SOW. All services delivered by DoIT under this agreement are done on a 100% reimbursable model and therefore costs will be billed accordingly to deliver that service.

VII. Termination of Service

This service will terminate at the completion of the date(s) identified in the SOW.

VIII. Warranty, Limitations, and Exclusions

A. Outlined accordingly in the SOW.