SERVICE ORDER ATTACHMENT

STATEMENT OF WORK

S-266-3148 LEVEL 3- MAST WEB APPLICATION TESTING

1 OVERVIEW

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement that incorporates this document by reference.

1.1 Service Summary

The purpose of Web Application Penetration Testing (the "Service") is to identify the feasibility of an attack on a Customer's Internet-facing web application(s) and to determine the extent of the impact of successful exploitation of that intrusion. The testing will employ intrusion analysis and testing methodologies to test the potential for successfully exploiting weaknesses within your web-based applications. The process will mimic typical attacker techniques and actual attempts to exploit web application vulnerabilities.

SilverSky web application penetration testers will meet with key members of the Customer's staff to determine the scope and 'rules of engagement' for performing the testing according to the list of potential in-scope activities listed below. This includes finalizing expectations and determining specific aspects such as the extent and depth of testing, notification requirements, and the timing of testing. All web application testing is performed remotely with minimal time commitment from the customer during the testing phases. If any critical vulnerability is identified, SilverSky's testing team will notify the Customer's main point of contact as soon as possible while the testing is in process.

1.2 In-Scope Service Details

SilverSky's Level 3 Web application service consists of a comprehensive manual review of a customer's web application. Manual web application penetration tests are considered a more thorough and in-depth form of testing compared to automated tools, as they cover a wider range of security issues and consider the unique design and implementation of each web application. Manual pen tests are security assessments that rely predominantly on the human element. Most test cases revolve around testing and evaluating a web application's business logic to identify potential security vulnerabilities.

The scope of the testing will be adjusted based on specific needs and time allotted for the project, but it may include the following options:

- Authenticated or unauthenticated testing
- Web application or mobile application testing
- API testing
- Infrastructure testing
- Customized technology testing available (IoT, OT, hardware, physical onsite, etc.)
- Timebox or comprehensive level of effort

1.3 Project Summary

SilverSky will provide the following primary tasks, subject to modification or extension based on the engagement.

1. Kick-off Meeting
2. Manual Application Security Testing (MAST)
3. Exploitation and Vulnerability Validation
4. Analysis of Findings
5. Draft Report and Review of Initial Findings
6. Final Comprehensive Report

1.4 SilverSky Methodology:

Kick-off Meeting – The purpose of the kick-off call is to discuss and agree on customer goals and the rules of engagement for the project. This includes project scoping (determining the target systems to be included in the testing), testing style (authenticated versus unauthenticated and the privilege level of authentication for users provided), the timeframe for testing, the extent to which system exploits can be performed, and procedures to follow should any issues occur during the testing. Any additional precautions or provisions are also considered before testing.

Manual Application Security Testing (MAST) – SilverSky will perform manual testing of the application revolving around testing and evaluating the web application's business logic to identify potential security vulnerabilities. Based on the scope identified in the kickoff call, this may involve authenticated testing into the application, review and testing of APIs within the application, and any customized testing based on the application's unique logic and structure.

Vulnerability Validation - SilverSky will make a best effort to validate findings from the application vulnerability scan manually. SilverSky processes and techniques for manual validation will vary significantly depending on the type of weakness identified but may include screenshots, manually verifying ports and protocols, or vulnerable versions in use. SilverSky will perform testing only under the agreed-upon rules of engagement.

Analysis of Findings Phase – SilverSky will compile and analyze the data generated from the assessment tools and manual checks and categorize vulnerabilities by severity, depending on the potential impact each can have on the affected network. This analysis is the basis for recommendations to potentially address risks associated with vulnerabilities.

Draft Report and Review of Initial Findings

At the conclusion of the assessment, SilverSky will provide a comprehensive draft report composed of an executive summary and a detailed findings section. The customer will have an opportunity to review drafts of the report and make any comments on the findings.

Final Report Delivery

SilverSky will deliver a final version after a joint review with the Customer, and any changes will be addressed from the draft report.

- Comprehensive Report detailing
    - Methodology followed.
    - Successful exploitation of the web application
    - Detailed recommendations for improvements

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope.

- Any web applications not identified as in-scope
- Any APIs or Infrastructure components not identified as in-scope
- Any retesting of the application after remediations are addressed unless specifically included in the SOW scope.
- Any testing not outlined in the in-scope testing section

If the Customer requests additional services, such services will be the subject of a change request.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

Services, fees, and work schedules are based on the assumptions, representations, and information supplied by the Customer. Customer's fulfillment of these responsibilities is critical to the success of the engagement.

2.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize the completion of key project phases, assign resources and serve as project liaison
- **Access** - Ensure SilverSky consultants have access to key personnel and data requested
- **Resources** - Furnish SILVERSKY with Customer personnel, facilities, resources and information and perform tasks promptly
- **Cooperation** - Ensure all of the Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer that increased Customer participation is required for SilverSky to perform the Service under this SOW.
- **Documentation** – Deliver in a timely fashion all documentation requested by SilverSky, including Customer's security policies, network diagrams, server listings, and procedures

2.2 SilverSky Assumptions

- Customer will provide SilverSky with reasonably requested information upon which SilverSky can rely to be current, accurate, and complete.
- Customer will provide access to Customer's personnel with detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who understand Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky deliverables and immediately notify SilverSky of any perceived problems or issues with SilverSky obligations.
- SilverSky will immediately notify the Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky cannot perform the Service due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

3 PROJECT PARAMETERS

3.1 Project Scope

The scope of the project is based on the above description with the additional details listed as follows:

Project Component	**Parameter(s)**
Project Start Date	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	Approximately 2-4 weeks, subject to project variables; comments on findings preliminary to comprehensive report to be delivered to SilverSky within 30 days of receipt of the initial report
Project Scope -Level 3 Manual Code Testing Tier 1	Web App Penetration Testing – Static Code Testing up to 80 hours of testing.
Project Scope -Level 3 Manual Code Testing Tier 2	Web App Penetration Testing – Static Code Testing up to 120 hours of testing.
Project Scope -Level 3 Manual Code Testing Tier 3	Web App Penetration Testing – Static Code Testing up to 160 hours of testing.

3.2 Location and Travel Reimbursement

The Services defined in this SOW may require onsite participation by SilverSky staff at Customer location(s) depending on the type of testing required. If onsite participation is required, additional charges will be billed for reimbursement.

3.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW. All deliverables will be marked with a Draft designation until final payment is received by the customer.