SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2166 WEB APPLICATION PENETRATION TESTING

1 OVERVIEW

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement which 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 Customer's Internet-facing web application(s) and to determine the extent of impact of a successful exploitation of that intrusion. The testing will employ intrusion analysis and testing methodologies to test the potential for Internet-based penetration of the systems. The process will mimic typical attacker techniques and actual attempts to exploit identified vulnerabilities. SilverSky consultants will meet with key members of Customer's staff to determine the scope and 'rules of engagement' for performing the testing. This includes clarifying or determining specific aspects such as the extent and depth of testing, notification requirements, and the timing of testing. The testing is performed remotely from the SilverSky offices. Typically, there is minimal interaction required of the Customer after the initial meeting.

Project Deliverables:

- Comprehensive Report

1.2 Project Summary

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

1. Kick-off Meeting
2. Information Gathering/Discovery
3. Security/Vulnerability Testing
4. Penetration Testing
5. Analysis of Findings
6. Report of Initial Findings
7. Report Review and Retesting (as indicated by initial results)
8. Comprehensive Report

1.3 SilverSky Obligations:

Kick-off Meeting - Meet personnel to discuss and agree upon the rules of engagement for the project. This includes project scoping (determining the target systems to be included in the testing), 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.

Information Gathering Phase - Use a variety of different reconnaissance techniques and processes to gather information about the target systems and understand the target environment and the types and versions of systems and applications in use. This includes domain research, port and service scans, fingerprinting and enumeration of systems.

Security Testing Phase - Assess the integrity and overall level of external security of critical network components such as servers and devices. SilverSky performs vulnerability scans using tools that are continually updated and contain checks for over thousands of known vulnerabilities and exploits.

1. **Perform ping sweep** - Automated ping sweeps of targeted IP addresses and network blocks to determine which addresses are connected to live systems and are responding.
2. **Perform port scan** – Scan for well-known TCP and UDP ports.
3. **Run assessment tools -** A variety of methods and techniques are used during this phase to assess the integrity and overall level of security of the web application; vulnerability scans, web configuration analysis, manual checks, and intentional errant data entry, among other tasks, are performed on the target website or web application. Consideration is given to the nature of the testing and the equipment being tested to ensure that little to no disruption is caused to the target system. In addition, SilverSky utilizes industry standard commercial and open source tools that are widely accepted and regarded in the security industry. No proprietary tools or applications are utilized.
4. **Perform manual checks** - Manually probe to confirm the validity of vulnerabilities and risk reported from the automated scans and to eliminate false positives. Manual checks also uncover vulnerabilities not identified by the assessment tools.

Penetration Testing Phase – Attempt to prove the ability to exploit a given vulnerability through validation that vulnerability could be successfully exploited. Validation of vulnerabilities is done as an alternative to full exploitation attempts and is a safer way to test the exploitability of system weaknesses especially on production systems. SilverSky processes and techniques will vary significantly depending on the type of weakness identified and may include activities such as testing if the system is exposed to sending malformed URLs and input on a website form, connecting to management services using default or cracked credentials, or checking the potential for running exploit code, among others. 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 in the affected network. This analysis is the basis for recommendations to potentially address risk associated with the vulnerabilities.

1.4 Deliverables

At the conclusion of the assessment, SilverSky will provide a comprehensive report composed of an executive summary and a detailed findings section. Customer will have an opportunity to review drafts of the report and SilverSky will deliver a final version after joint review with Customer.

Executive Summary - The executive summary summarizes the results of the assessment. It is intended for upper management and boards of directors and includes:

- Overview of assessment results
- Itemization of the risk ratings for each area reviewed during the assessment
- Key findings and recommendations

Detailed Findings - The detailed findings section describes the assessment results in detail. It is intended for management, administrators, and other operations personnel and includes:

- An itemized listing of individual vulnerabilities
- A description of each vulnerability
- The severity of the threat likely posed by each vulnerability
- Potentially affected resources
- Recommendations for remediation

1.5 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. In the event that Customer requests additional services, such services will be the subject of a change request.

2 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

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

2.1 Customer Obligations

- **Project Liaison** - Designate an authorized representative to authorize 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 Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise Customer increased Customer participation is required in order 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 who have detailed knowledge of Customer security architecture, network architecture, computing environment, and related matters.
- Customer will provide access to Customer's personnel who have an understanding of 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 Customer of any perceived problems or issues regarding Customer obligations.
- Customer is responsible for any additional costs if SilverSky is unable to 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	Typically within 30 days of Effective Date
Project Duration	Approximately 2-3 weeks, subject to project variables; comments on findings preliminary to comprehensive report to be delivered to BAE within 30 days of receipt of initial report
S-266-2166 – Web App Penetration Testing (advanced)	• External Web App Penetration Testing of up to 2 Web Application Architecture (up to 10 servers/host architecture) • Authenticated and Unauthenticated checking with customer provided credentials • Includes system validation of penetration testing results. No live exploitation will be performed on production systems
S-266-2166 – Web App Penetration Testing (core)	• External Web App Penetration Testing of 1 Web Application Architecture (Up to 5 servers/hosts for assessment) • Authenticated and Unauthenticated checking with customer provided credentials • Includes system validation of penetration testing results. No live exploitation will be performed on production systems

3.2 Location and Travel Reimbursement

The Service defined in this SOW may require onsite participation by SilverSky staff at Customer location(s).

For Customer approved on-site participation, Customer will be invoiced for all actual SilverSky staff travel and living expenses associated with all on-site visits. An administration fee of ten percent (10%) of all travel and living expenses will be billed to Customer in the event Customer requires an itemized statement of such expenses.

Location	**Scope of Work**

3.3 Acceptance

Delivery of all stated project deliverables will constitute acceptance of services provided under this SOW.