SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2721 INTERNAL VULNERABILITY ASSESSMENT

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 the Internal Vulnerability Assessment Service (the "Service") is to analyze, assess, and test the overall integrity of the Customer's internal network and critical information technology assets in order to uncover and identify potential security weaknesses and flaws.

SilverSky will analyze these areas against generally accepted industry standards and practices. Following the assessment, SilverSky will provide an overview of results detailing the identified vulnerabilities or deficiencies and recommended steps to potentially remediate or mitigate the associated risk(s).

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 Testing
4. Analysis of Findings
5. Reporting

2 SCOPE

2.1 SilverSky Obligations:

Information Gathering Phase - Meet with key Customer staff to gain an understanding of the environment and network. SilverSky gathers existing network documentation such as server listings, network diagrams, device configurations, and network application listings, and examines documentation related to the Customer's information security program, formal information risk assessment, and disaster recovery plan.

Security Testing Phase - Assess the integrity and overall level of internal security of critical network components such as servers and devices. Perform vulnerability scans using tools that are continually updated and contain checks for 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 vulnerability assessment tools** - Scan the network range utilizing specialized security software packages representing thousands of known vulnerabilities. These scans probe communication services, operating systems, applications, and systems.
4. **Perform manual checks** - Manually probe to confirm the validity of vulnerabilities and risks reported from the automated scans and to eliminate false positives. Manual checks also uncover vulnerabilities not identified by the assessment tools.

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 risks associated with the vulnerabilities.

2.2 Deliverables

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

2.3 Out of Scope

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

3 CUSTOMER OBLIGATIONS AND ASSUMPTIONS

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

3.1 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 the Customer if 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

3.2 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 the 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.

4 PROJECT PARAMETERS

4.1 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 the Effective Date
Project Duration	Approximately 2-4 weeks, subject to project variables
S-266-2721 Internal Vulnerability Assessment Tier 2	Up to 500 IP addresses in scope. Work hours not to exceed 45
S-266-2721 Internal Vulnerability Assessment Tier 1	Up to 100 IP addresses in scope. Work hours not to exceed 30

4.2 Location and Travel Reimbursement

The Service defined in this SOW may require on-site participation by SilverSky staff at customer location(s).

For Customer approved on-site participation, the 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 the Customer in the event the Customer requires an itemized statement of such expenses.

Location	**Scope of Work**

4.3 Acceptance

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