SERVICE ORDER ATTACHMENT

STATEMENT OF WORK

S-266-3151 NIST 800-53 MATURITY ASSESSMENT

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 Services Summary

The SilverSky NIST 800-53 Maturity assessment aims to identify potential gaps in the Customer's ongoing security program and compliance efforts. The assessment procedures are based on the latest NIST 800-53 Moderate Standards as updated by the National Institute of Standards and Technology. This project will focus on Customer policies, procedures, practices, information technology (IT) environment, and existing compliance efforts. SilverSky will document and assess the client's controls to identify areas of weaknesses or missing controls and provide recommendations to help the Customer enhance its security and compliance program.

Project Deliverables:

- Reports: Executive Summary and Maturity Detailed Findings Report

1.2 Project Summary

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

1. Preparation and Scoping
2. Information Gathering/Discovery
3. Maturity Analysis
4. Analysis and Reporting

2 Scope

2.1 SilverSky Obligations:

Preparation and Scoping - Meet with key personnel to discuss the Customer's operational and technical environment. During this initial conversation, SilverSky will assess the Customer's IT environment, including considerations for outsourced arrangements, network segmentation, and third-party providers. This preparation and scoping phase is used to:

- Set expectations regarding the project scope, objectives, activities, and associated timetables throughout the engagement
- Establish roles and responsibilities for both Customer and SilverSky teams
- Validate customer requirements against the NIST 800-53 Medium standards
- Establish project management standards, including milestone meetings, status reports, and ongoing communications with key personnel
- Facilitate the collection of Customer specific information that is required to complete the gap assessment

Information Gathering – Assess and review existing Customer documents related to NIST 800-53 compliance and interview Customer personnel. SilverSky will perform interviews and review of documentation provided by the client throughout the review process. Samples of requested documentation will include:

- Prior IT or Operation risk assessments
- Network diagrams
- Security and compliance training programs
- Information security policies and procedures
- Workforce training program documentation
- IT organizational charts
- Security software and hardware lists
- Interview schedules with key personnel

SilverSky will utilize the information gathered to focus better and streamline the client interviews. SilverSky will schedule group and individual interviews with personnel from various functional areas. The interview process will focus on the areas outlined in the NIST 800-53 security standard.

Gap Analysis - Evaluate the in-scope processes, systems, and applications against the NIST 800-53 security requirements. SilverSky will examine the security and control structure or related information systems and business processes involved in the Customer's collection, use, and disclosure of credit card data to determine their compliance. During this phase, SilverSky will:

- Interview key system and business stakeholders to identify current policies and practices related to credit card data
- Identify and assess information security risks within key functional areas
- Understand current risk management techniques for addressing security and privacy risks
- Identify deficiencies and gaps in the security practices through control analysis
- Develop detailed recommendations to assist Customer's remediation of deficiencies

SilverSky will review these domains for compliance with the 20 control families listed in the NIST 800-53 standard:

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment, Auth and Monitoring
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Privacy Authorization
- Physical and Environmental
- Planning
- Program Management
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

Analysis and Reporting—Analyze the data generated from the SilverSky review. SilverSky will categorize the gap analysis by severity depending on the potential impact each gap may have on compliance with the NIST 800-53 security standard. SilverSky will make recommendations to help the Customer formulate a strategic plan to address any non-compliant areas.

2.2 Deliverables

SilverSky will provide an Executive Report and a Detailed Findings Report following its review.

The Executive Report is a high-level summary of the review designed for Customer's upper management and board of directors and includes:

- 1-page executive summary
- Concise list of the key findings
- Summary of findings for each area reviewed during the review
- High-level recommendations for addressing deficiencies

The Detailed Findings Compliance Gap/Readiness Report outlines the current control status against NIST 800-53 requirements and describes areas of missing controls. It's designed for mid-level management, administrators, and other operations personnel and includes:

- Itemized listing and description of the areas reviewed
- Identified deficiencies
- Overall risks associated with deficiencies
- Detailed recommendations for addressing deficiencies

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If 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. 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 completion of key project phases, assign resources and serve as project Liaison.
- **Access** - Ensure SilverSky's consultants can access key personnel and requested data.
- **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 and in a timely manner with SilverSky. SilverSky will advise the Customer if an increased level of Customer participation is required for SilverSky to perform the Service.
- **Documentation** - Timely deliver 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 accurate and complete.
- Customer will provide access to personnel with detailed knowledge of the Customer's security architecture, network architecture, and compute environment.
- Customer will provide access to its personnel who understand the Customer's security policies, regulations, and requirements.
- Customer will evaluate SilverSky's 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 Services 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	SilverSky will reach out within 30 days of the Effective Date with a date for a kickoff call.
Project Duration	NIST 800-53 Moderate: Approximately 2-3 weeks
S-266-3151 NIST 800-53 Maturity Assessment – Moderate Baseline	Up to 120 hours, Assessment against Moderate Baseline

4.2 Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely; no onsite travel is required for this engagement.

4.3 Acceptance

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

[End of Document]