SERVICE ORDER ATTACHMENT

STATEMENT OF WORK

S-266-2902 NIST 800-171 GAP/READINESS REVIEW

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 Services Summary

The purpose of the SilverSky NIST 800-171 Gap assessment is to identify potential gaps that may exist in Customer's ongoing security program and compliance efforts. The assessment procedures are based on the latest NIST 800-171 Security Standards as updated by the National Institute of Standard and Technology. This project will focus on Customer policies, procedures, practices, information technology (IT) environment and existing compliance efforts. SilverSky will document identified weaknesses and provide recommendations to help Customer enhance its security and compliance program.

Project Deliverables:

- Reports: Executive Summary and GAP/Readiness 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. Gap Analysis
4. Analysis and Reporting

2 Scope

2.1 SilverSky Obligations:

Preparation and Scoping - Meet with key personnel to discuss Customer's operational and technical environment. During this initial conversation, SilverSky will assess the make up of 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 over the course of the engagement
- Establish roles and responsibilities for both Customer and SilverSky teams
- Establish project management standards, including milestone meetings, status reports and ongoing communications with key personnel
- Facilitate collection of Customer specific information that is required to complete the gap assessment

Information Gathering - Review existing Customer documents related to NIST 800-171 compliance and interview Customer personnel. SilverSky may require further interviews and documentation 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 better focus and streamline the client interviews. SilverSky will schedule a combination of group and individual interviews with personnel from various functional areas. The interview process will focus on the areas outlined in NIST 800-171 security standard.

Gap Analysis - Evaluate the in-scope processes, systems and applications against the requirements of the NIST 800-171 security requirements. SilverSky will examine the security and control structure or related information systems and business processes that are involved in 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 14 control families listed in the NIST 800-171 standard:

- Access Control
- Media Protection
- Awareness and Training
- Personnel Security
- Audit and Accountability
- Physical Protection
- Configuration Management
- Risk Assessment
- Identification and Authentication
- Security Assessment
- Incident Response
- System and Communications Protection
- Maintenance
- System and Information Integrity

Analysis and Reporting - Analyze the data generated from SilverSky review. SilverSky will categorize the gap analysis by severity depending on the potential impact each gap may have with respect to compliance with the NIST 800-171 security standard. SilverSky will make recommendations to help 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 Report describes the review results in detail. 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. In the event that Customer requests additional services, such services will be the subject of a change request.

3 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.

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 SILVERSKYS consultants have access to key personnel and data requested.
- **Resources** - Furnish SILVERSKYS with Customer personnel, facilities, resources and information and perform tasks promptly.
- **Cooperation** - Ensure all of Customer's employees and contractors cooperate fully with SILVERSKYS and in a timely manner. SilverSky will advise Customer if an increased level of Customer participation is required in order for SILVERSKYS to perform the Services under this Service Description.
- **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 Customer's personnel who have detailed knowledge of Customer security architecture, network architecture, compute environment and related.
- Customer will provide access to Customer's personnel who have an understanding of Customer's security policies, regulations and requirements.
- Customer will evaluate SILVERSKYS 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 in the event that SilverSky is unable to 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	Typically within 30 days of Effective Date
Project Duration	Tier 1: Approximately 1-2 weeks Tier 2: Approximately 2-3 weeks Tier 3: Approximately 3-4 weeks
Description	Consulting Days not to Exceed
800-171 Compliance GAP/Readiness Review - Tier 1	7
800-171 Compliance GAP/Readiness Review - Tier 2	12
800-171 Compliance GAP/Readiness Review - Tier 3	20

Pricing is based upon your Tier of service and you are not allowed to downgrade if the engagement last less than your maximum days set forth in the table above.

4.2 Location and Travel Reimbursement

The Services defined in this SOW may require onsite participation by Silversky staff at customer location(s).

For Customer-approved onsite participation, Customer will be invoiced for all actual SILVERSKYS staff travel and living expenses associated with all onsite visits. An administration fee of ten percent (10%) of all travel and living expenses will be billed to Customer if 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.

[End of Document]