SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-2715 CISO ADVISORY SERVICE ANNUAL PROGRAM

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

SilverSky will assist Customer by providing strategic program direction, oversight and guidance towards building and maintain a cyber security program throughout the year. This service is intended to be a program with several key objectives and milestones to assist the customer in the development of a cyber resilient security program. During the year, SilverSky will assess several phases which are critical in developing a security program. After performing the review, Silversky will assist Customer in developing a comprehensive security program within the missing areas, provide program oversight and report the status of the program to executive leadership and the board of directors. SilverSky will utilize established security standards such as NIST, COBIT and ISO 27001 as well as any industry specific regulations pertinent to the customer as benchmarks for the program development and CISO advisory work.

Project Deliverables:

- Reports: Executive Report and Detailed Program Documentation

1.2 Project Summary

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

- Phase 1 – (Month 1) – Strategy and Governance Overview
- Phase 2 – (Month 2-4) – Initial Program Review and Assessments -
- Phase 3 – (Month 4-8) – Program Development
- Phase 4 – (Month 8-12) - Oversight and Continuous Monitoring

2 Scope

2.1 SilverSky CISO Advisory Obligations:

The CISO Advisory services rely on the full cooperation and participation of Customer to complete any prescribed interviews, walkthroughs, and questionnaires.

Strategy and Governance – Interview the customer to Identify business threats, understand customer's unique risk profiles, baseline current security program, and define security strategy in line with business objectives and technology strategies. Any existing Information security program-related documentation will be gathered and examined. This documentation includes, but is not limited to, the following: information security policies and procedures, network diagrams, results from prior assessments or reviews, vendor agreements and recovery plans. The documentation is reviewed in detail and used to identify areas that might require additional focus or attention.

Initial Program Review and Assessments – SilverSky will evaluate the security program from the people, processes and technologies that make it up to determine potential gaps and then help to develop a strategic plan of prioritized actions to improve your information security strategy and program. Assessments may include in depth reviews of cyber program areas including but not limited to:

- Interviews with stakeholders
- Review of existing policy sets
- Cyber Risk Management
- Cyber Control Evaluations
- Cyber Maturity Assessments
- Incident Detection and Response Capabilities
- Third Party Risk and Oversight
- Vulnerability Management Programs
- Compliance Reviews

- Policy and Procedure Reviews
- Reviewing Risk Management Strategy

Development Phase – SilverSky will assist in developing the security program in the following key program areas:

1. **Security Architecture** – SILVERSKYS will make strategic recommendations for improving the security architecture within the areas of design, setup, and layout. Recommendations will be based on commonly held standards in respect to security and compliance with industry best practices.

2. **Security Administration** -The objective of the administration development is to help document policies and procedures within key areas of a security program. The development considers common security standards as well as any particular regulatory requirements the organization might be required to comply with. The development of the program does not include solution-oriented costs, managed service fees or any other fees associated with the technology or services to operate the program.

   The development typically addresses the following critical areas:

   - Security policy development
   - Security roles and responsibilities
   - Risk assessment process
   - Incident Response Plan development
   - Development of End user security training program
   - Development of vulnerability management program
   - Development of Vendor/third party management program

Continuous Monitoring and Oversight - Based on the outcome of the development phase, SilverSky's CISO advisory services can help support the maturity and maintenance of your cyber program through various program oversight initiatives, such as performing continuous evaluation and oversight of the following key functions:

- Email security
- Network security monitoring
- Incident response program
- Physical security
- Device security
- End point controls
- Anti-virus
- Wireless and mobile security
- Risk Management
- Third Party Oversight
- Vulnerability and patch management

2.2 Deliverables

SilverSky will provide a Detailed Findings Documentation following any assessment.

SilverSky will provide program documentation including policies and procedures when developing any program item.

The Detailed Program Documentation will include items required to help Customer document its security program. These items vary by the needs of Customer and may include:

- Policy documentation
- System standards
- Control recommendations
- Procedural documents
- Response plans

SilverSky will provide findings and recommendations as part of the oversight of the program and strategic recommendations for improvement.

SilverSky will provide board level and executive summary reports for any committee or Board meeting on a quarterly basis

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

- 1 page executive summary
- Concise list of the key findings and recommendations grouped according to these asset categories:
    - Information Systems - applications such as data processing, reporting, websites
    - Information Technology - equipment such as servers, workstations, firewalls
    - Physical Information - items such as hard copy reports, backup tapes
- Comprehensive information security plan detailing recommended safeguards and processes
- Recommended schedule for performing and testing specific controls

2.3 Out of Scope

Any activity not explicitly included in this SOW is considered out of scope. If Customer requests additional services, such services will be the subject of a change request. Managed Services and ongoing operations of any program items is not included in scope and will be outlined on a separate SOW.

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 SilverSky consultants have access to key personnel and data requested - to include access to critical IT assets, systems and physical locations such as server rooms, data centers, and operations facilities
- **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 if an increased level of Customer participation is required in order for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely deliver all documentation requested by SILVERSKYS-- including Customer's security policies, prior security reviews, 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, computer environment and related infrastructure.
- 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 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

4.2 Location and Travel Reimbursement

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

For Customer-approved onsite participation, Customer will be invoiced for all actual SilverSky's 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.

4.3 Acceptance

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

[End of Document]