SERVICE ORDER ATTACHMENT
STATEMENT OF WORK

S-266-3285 SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM DEVELOPMENT

Overview

This Statement of Work ("SOW"), with any appendices included by reference, is part of any agreement that incorporates this document by reference.

Services Summary

The SilverSky Supply Chain/Third Party Risk Management (SCRM) Program Development assists the Customer in developing and/or updating its Supply Chain Risk Management program. This service consists of SilverSky performing an initial baseline understanding of the customer's current SCRM program. Once a baseline is established, SilverSky will help build the customer's SCRM framework by addressing gaps in the existing program or starting with a new framework. SilverSky will provide the tools, strategy, and consulting guidance to develop a baseline Supply Chain Risk Management program aligned with the key requirements in the NIST Cybersecurity Framework and NIST IR 8276.

Project Summary

SilverSky will collaborate with Customer to execute the project tasks and provide regular updates throughout the project, subject to modification or extension based on the engagement.

1. Kickoff Meeting and Initial Program Review
2. Supply Chain Risk Management Charter Documentation Development
3. Third Party Supply Chain Policy and Standard Operating Procedure Development
4. Development of the Supply Chain Risk/Third Party Risk Assessment Document
5. Development of a Key Supplier assessment questionnaire
6. Final Review and Out brief

Deliverables

- Supply Chain Risk Management Framework, tools, templates and customization.

Scope

SilverSky Obligations:

SilverSky will collaborate with Customer to execute the project tasks and provide regular updates throughout the project.

1. Kickoff Meeting and Initial Program Review

The SilverSky consulting team and Customer stakeholders will meet to discuss:

- Introductions
- Points of Contact
- Scope of Work
- Overview of Existing Program
- Meeting and Resource Scheduling

2. Supply Chain Risk Management Charter Documentation Development

NIST CSF and IR 8276 require that the development of a Supply Chain Risk Councils that include executives from multiple internal departments be part of the third-party risk committee. Required activities include meeting

regularly to review relevant risks and mitigation plans, set priorities, drive the sharing of best practices across the enterprise, and pilot initiatives. SilverSky will assist the customer in drafting the Supply Chain Risk Charter. This document will outline the council's purpose, membership, meeting frequency, and other requirements. The Customer will staff the Council membership and conduct ongoing meetings as part of the program.

3. **Third Party Supply Chain Policy and Standard Operating Procedure Development**

During this phase, SilverSky will draft a supply chain risk management policy aligned with NIST SCRM requirements. NIST SCRM requires a formal C-SCRM program and policy structure within the organization that outlines organizational accountability for managing cyber supply chain risks. The policy will outline the requirements to maintain a SCRM. In addition, SilverSky will help develop a standard operating procedure document that outlines the functional requirements that must exist within the program.

4. **Development of the Supply Chain Risk/Third Party Risk Assessment Document**

SilverSky will provide the customer with the templates and work programs needed to perform an initial SCRM/Third Party risk management assessment of their critical vendors in compliance with the NIST SCRM requirements to know and manage their critical suppliers. The assessment work program will allow the customer to identify and rank their supply chain based on risk criteria set out in the work programs. The SilverSky consultant will help perform the risk assessment on the first 3 vendors as part of a knowledge transfer for the customer. The customer will ultimately be responsible for completing the assessment on the remaining vendors and performing ongoing risk assessments of new vendors.

5. **Development of a Key Supplier assessment questionnaire**

As part of the final phase of a SCRM program, the NIST guidance requires organizations to perform ongoing assessments and monitor throughout the supplier relationship. SilverSky will assist with the development of a Key Supplier questionnaire that can be sent to key vendors on an ongoing basis to assess their compliance with the Supplier Security Program. It is ultimately up to the customer to manage the sending, receiving, and evaluation of the questionnaire as part of the maintenance of the program.

6. **Final Review and Out brief**

A final review meeting will be held after the SCRM Framework and documents have been created. This meeting will showcase these documents and, in addition, discuss anything notable observed during the discovery or evaluation processes. SilverSky will provide a final round of revisions before finalizing and delivering the documents to Customer.

Project Deliverables

The SCRM Plan deliverables consist of the following:

- SCRM Charter Documentation
- SCRM Policy Document
- SCRM Standard Operating Procedure
- SCRM Risk Assessment Work Program
- SCRM Vendor Questionnaire

SilverSky will deliver the agreed-upon information or documents as defined under the above Project Parameters section.

Out of Scope

The following Activities are out of scope for this service:

- Establishing SCRM Charter Memberships
- Performing SCRM risk assessments and rankings beyond the initial 3 provided as a starting point
- Policy and standard operating procedures above and beyond that stated in the SCRM service description.
- Sending, receiving, or assessing SCRM risk assessment questionnaires
- Ongoing running or Maintenance of the customer's SCRM program beyond the initial development work
- Any activity not explicitly included in this SilverSky Obligation section of this SOW is considered out of scope.

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 engagement's success.

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 Customer's employees and contractors cooperate fully with SilverSky and in a timely manner. SilverSky will advise the Customer if an increased level of Customer participation is required in order for SilverSky to perform the Services under this SOW.
- **Documentation** - Timely delivery of all documentation requested by SilverSky, including Customer's security policies, network diagrams, server listings and procedures.
- SilverSky Assumptions

Customer will provide SilverSky with reasonably requested information that SilverSky can rely on as current, accurate, and complete.

- Customer will provide access to Customer's personnel who have detailed knowledge of Customer's security architecture, network architecture, computer environment and related infrastructure.
- Customer will provide access to Customer's personnel who understand Customer's security policies, regulations and requirements.

The 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 Services due to Customer's delay or other failure to fulfill its obligations under this Statement of Work.

Project Parameters

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 1 week, subject to project variables
SCRM Program Development	Work hours not to exceed 40 hours

Location and Travel Reimbursement

The Services defined in this SOW will be performed remotely.

Acceptance

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

[End of Document]