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.

- 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

2.1 SilverSky Obligations:

- Meet with key personnel to discuss Customer's operational and technical environment. During this initial

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

- 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

- Itemized listing and description of the areas reviewed
- Identified deficiencies
-

V 2023-07-25 © 2023