PROFESSIONAL SERVICES
SECURITY RISK ASSESSMENT (NIST 800-171)
STATEMENT OF WORK
TO VERIZON PROFESSIONAL SERVICES SERVICE ATTACHMENT

This Statement of Work (SOW) is entered into between the entities identified as, respectively, Verizon and Customer in the related Service Order Form (SOF).

1. **PROJECT DESCRIPTION.** Verizon will provide Customer with a Security Risk Assessment (SRA) using National Institute of Standards and Technology (NIST) 800-171 standards. Customer may also order a Roadmap option which provides guidance on implementing Verizon's recommendations.

2. **SCOPE OF WORK.** Verizon's SRA service will be provided an assessment of Customer's security requirements in the functional areas listed in the NIST 800-171 standard as provided below (Security Requirements):

NIST 800-171		
• Access Control • Awareness and Training • Incident Response • Risk Assessment • Security Assessment	• Identification and Authentication • System and Communications Protection • System and Information Integrity • Audit and Accountability	• Maintenance • Media Protection • Personnel Security • Configuration Management • Physical Protection

2.1 **Package Sizes.** SRA is available in Small, Medium, and Large sizes (Customer selected size detailed on the SOF). Small package is for companies with less than 1,000 employees, one local headquarter (HQ) location and one primary local business unit, with risk assessment for up to five environments. Medium package is for companies with less than 10,000 employees, one local HQ location and up to three primary local business, with risk assessment for up to ten environments. Large package is for companies with greater than 10,000, and no more than 50,000 employees, one local HQ location and up to four primary business units (international locations will be delivered remote only) with risk assessment for up to fifteen environments. Packages will be delivered locally which means in the same country as the contracting country, except where specifically stated.

2.2 **Project Initiation**. Verizon will schedule and conduct a kick-off meeting to initiate the Project, to review the SRA size ordered, and confirm if the Order includes Roadmap option. Verizon and Customer will identify business systems to be assessed, as well as documentation and responsible individuals with knowledge of Customer's business systems and security protections. Verizon will review Customer documentation, and will work with Customer to plan interviews.

2.3 **Data Collection**. Verizon will review Customer provided documentation, interview identified individuals and collect information regarding Customer's business systems and security protections.

2.4 **Data Analysis**. Verizon will analyze the collected information and determine Customer's information security protection maturity, performance, and scope relative to Customer's Security Requirements. Verizon will perform threat analysis and business impact analysis of the identified business systems. Using the threat and business impact analysis, Verizon will develop an information security risk rating for each of the identified business systems. This will result in a customized analysis of threat actors and threat actions that are most likely to compromise the identified business systems, along with the business impact associated with the compromise of the business systems. Verizon will develop and rank order conclusions

and recommendations designed to help Customer avoid or reduce risks, and/or achieve greater alignment with Customer's Security Requirements.

2.5 **Roadmap**. If ordered pursuant to a SOF, Verizon will provide a detailed roadmap for implementing Verizon's recommendations in the report. Verizon will meet with Customer to determine which recommendations from the report will be included in the Roadmap and then develops project definitions, timing, costs and staffing projections for each recommendation that is to be included in the Roadmap.

2.6 **Security Assessment Program Report**. Verizon will develop a draft report and deliver it to the Customer via secure means. Customer will review the report and make comments, and Verizon will finalize and submit a final report to Customer. The final report will include the findings and recommendations (SRA Report). The SRA Report will include the following sections**:**

- Executive Summary**:** Highlights Customer's current Customer's information security risk based on the identified business systems and the Customer's information security protections relative to Customer's Security Requirement, and provides a summary of recommendations for improving Customer's information security protections.
- Controls Assessment**:** Provides Verizon's assessment of Customer's information security protections compared to Customer's Security Requirement. This includes analysis of the alignment and maturity of information security protections with each of the required information security controls.
- Risk Analysis. Provides a profile of identified business systems, threat analysis, business impact and the resulting information security risk associated with each system. This results in a series of tables, graphics and heat maps that show the likelihood, business impact and the risk of a breach of each system.
- Recommendations**:** Provides recommendations for improvements to Customer's information security protections that address identified weaknesses, and reduce the risk of a breach. Verizon provides a suggested priority order for implementing the recommendations to mature the information security program and reduce the risk to Customer.
- Roadmap**:** If purchased, provides a roadmap of Verizon's recommendations that includes project definitions, timing, estimated costs and staffing projections for each project that is to be included in the Roadmap.

2.7 **Project Management.** Verizon will designate a project manager who will act as the central point of contact throughout the Project. The project manager is also responsible for managing the change control process.

3. **DELIVERABLES.** Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Deliverables include the SRA Report.

4. **FINANCIAL TERMS.** Customer will pay the Charge as detailed in the SOF. Travel and expenses, if any, will be billed as provided in the PSSA, this SOW, and the SOF.