PROFESSIONAL SERVICES
REMOTE WORKING SECURITY ASSESSMENT
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 the Remote Working Security Assessment (RWSA). Verizon's RWSA service has two parts, a remote access environmental assessment, and a remote access VPN penetration test, each as further described below. All services will be performed remotely.

2. **SCOPE OF WORK.** Verizon's RWSA service will begin with a remote kick-off call. During the call, Verizon and Customer will identify documentation and responsible individuals relevant to Customer's accomplishment of Customer's security program. After the kick off call Verizon will begin to deliver the two parts of assessment, which may be performed concurrently, each as further described below.

2.1 **Remote Access Environmental Assessment.** Verizon will conduct a remote access environmental assessment, addressing the security areas listed below as the standard for this assessment (the Security Requirement). Verizon will focus on one (1) VPN platform and conduct remote interviews as applicable. Security areas include:

- Policies,
- Asset Management,
- Access Control,
- Remote Access,
- Logging & Monitoring,
- Configuration & Patch Management,
- Encryption, and
- Identity & Access Management.

Verizon will review Customer documentation collected from Customer during the kick off call, and will work with Customer to setup and conduct interviews to identify security controls that are not fully documented. Verizon will then analyze Customer's security program maturity, performance, and scope relative to the Security Requirements. Verizon will utilize ISO 27001/27002 to develop compliance and maturity scores from this analysis, and identify Customer's performance around Customer's Security Requirements. Verizon will develop and rank order conclusions and recommendations designed to help Customer avoid or reduce risks, and/or achieve greater alignment with their Security Requirements.

2.2 **Remote Access VPN Penetration Test.** Verizon will conduct a penetration test on Customer's remote access Virtual Private Networks (VPN) with the objective to identify security weaknesses that could be exploited by motivated malicious individuals to gain unauthorized access to the corporate internal infrastructure. When applicable, exploitation will be conducted to demonstrate the ability to gain unauthorized access to system resources and/or potentially disrupt VPN system services. Verizon will also attempt to emulate a legitimate VPN client system to attempt to connect an unauthorized system to the VPN. To perform some of these tasks, Verizon may require access to an authorized VPN client system as an unprivileged user. Verizon uses a series of vulnerability scanning tools and manual techniques to identify, validate, and exploit security vulnerabilities. Testing will include following three (3) phases:

2.2.1 **Unauthenticated External Bad Actor.** Verizon will perform black box testing, targeting the VPN head end/concentrator. Verizon will attempt to exploit vendor device vulnerabilities as well as misconfigurations, and depreciated or insecure encryption protocols being used. Customer credentials are not required to perform this exercise.

2.2.2 **Authenticated Bad Actor**. Verizon uses Customer provided credentials, such as a typical employee or contractor that has been phished or laptop stolen, for this exercise. The goal of this phase is to test access controls over the VPN as well as what information can be harvested from the client system and used to further the bad actor's access on the internal network. Verizon will review any pre and post authentication checks, such as Multi-Factor Authentication (MFA), certificates and Anti-Virus signature review, in an attempt to bypass all or part of the authentication process.

2.2.3 **VPN Client Access and Configuration Review.** Verizon, connected to the VPN using a Customer-provided VPN client system, will perform testing access controls and authorization pushed down to the user's VPN profile. Verizon will attempt to subvert access restrictions applied to them by the VPN in an attempt to access portions of the network not permitted by their VPN profile.

2.2.4 **Platform**. Verizon will perform the VPN Penetration Test on one (1) VPN platform with one (1) user role. Additionally, Verizon will perform a malicious user emulation test in an attempt to bypass access controls and gain access to sensitive resources not intended for use by the malicious user. For purposes of the SOW, 'platform' refers to the functional equivalent of a single VPN configuration, so that the assessment of two (2) VPN configurations on a single piece of hardware will be counted as the assessment of (2) VPN platforms

2.3 **Management Review.** After the environmental assessment and penetration test have been performed, Verizon will develop a draft report, deliver it Customer and will conduct a teleconference to explain Verizon's results to Customer. Customer will review the report and make comments, and Verizon will finalize and submit a final report to Customer.

2.4 **Project Management Approach.** 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. Should the Project's requirements change during the course of the Project, the project manager will ensure that any modifications to the SOW are agreed and documented in a mutually executed change order as an amendment to the SOW in accordance with the Professional Services Service Attachment.

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. Verizon will provide a report of findings and recommendations (Report). The Report will include:

- Executive Summary: Highlights Customer's current state as relative to its Security Requirements, and provides high-priority recommendations.
- Introduction: Describes the scope of the Project; summarizes Verizon's approach, identifies participants, locations and timeframes.
- Results: Provides Verizon assessment of Customer's security strengths and areas for Improvements as relative to Customer's Security Requirements, and discusses root cause issues around risks and compliance. For the VPN Penetration Test, the report outlines vulnerabilities identified by Verizon in order of severity. Each finding will include a discussion of the vulnerability and the potential security impact to the applications, as well as recommended remediation steps. Screen shots and log excerpts may be included, if applicable.
- Recommendations: Provides tactical and strategic recommendations in Verizon's suggested priority order, based on risk avoidance/reduction and compliance alignment to Customer's Security Requirements. 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.

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.