Threat Intel and Response Service Professional Service Description
Wireless Vulnerabiilty Assessment

1. **Scope of Work.**

1.1 **Wireless Vulnerabiilty Assessment.** The Project consists of wireless vulnerability assessment (the "Professional Services"). The Professional Services will identify and assess vulnerabilities in the networks, access points ("AP") and wireless clients associated with Customer IEEE 802.11a, 802.11b, 802.11g, and 802.11n wireless technology for Customer's service set identifiers ("SSIDs") at the locations requested by Customer and shown in the Engagement Letter (the "Targeted Location(s)").

Verizon will test the physical perimeter of Customer's wireless network(s) at the Target Location(s) and its use of encryption and authentication, search for rogue access points, and review access point configuration. Verizon will also examine how wireless clients are configured by Customer and secured against connection to rogue access points or hijackings over their wireless interface. Verizon's wireless security assessment will consist of the following phases:

1.1.1 **Discovery.** Verizon will identify and inventory wireless access points whose signal can be received at the Targeted Location(s), whether physically located at or nearby the Targeted Location(s). Additionally the Customer signal leakage will be mapped to determine the amount of bleed over outside the Customer Targeted Location(s).

1.1.2 **Wireless Penetration testing.** Verizon will attempt to establish unauthorized connections with those access points physically located at the Targeted Location(s). Verizon will first capture information from existing communications, such as private keys, SSIDs, usernames and passwords, and encryption schemes deployed. Next, Verizon will use the gathered information to attempt to establish an unauthorized wireless connection with the Targeted Location(s) access points, hijack an existing connection, break the encryption scheme in use, and/or impersonate a valid user. Additionally Verizon will attempt to assess the security of wireless client devices accessing the Targeted Location(s) wireless network by attempting man-in-the-middle attacks, false Customer access points, and other scenarios to ascertain the security of wireless client devices.

1.1.3 **Rogue Detection.** Verizon will walk through the Customer premises to identify and locate rogue access points and ad-hoc networks (those access points and networks not authorized by Customer) and then attempt to determine if they are connected to the Customers network.

The Professional Services will be provided onsite by Verizon, unless otherwise agreed.

1.2 **Project Management.** Verizon will work with Customer to schedule a kickoff meeting to initiate the Project. Verizon and Customer will collaborate to determine required stakeholders and other attendees, agenda, location, and whether the meeting will be on site or virtual. During or before the kickoff meeting, Customer shall provide a list of appropriate contact personnel with "after hours" emergency contact numbers, and appropriate on-site authorization documentation (where applicable). As an output of the meeting, Verizon will produce an agreed project plan, which specifies resources, dates, times, and locations for the tasks described (the "Project Plan").

2. **Deliverables and Documentation to be produced by Verizon (if any).** 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:

2.1 The Project Plan.

2.2 A report of findings that outlines discovered vulnerabilities in order of severity (the "Report"). Each finding will include a discussion of the vulnerability and the potential security impact to the mobile applications, as well as recommended remediation steps. Screen shots and log excerpts may be included, if applicable.

2.3 The Report will include an executive summary, which contains an analysis of the results of the Professional Services. The Report will include a description of Verizon's findings, and graphs and charts to break down findings by severity and difficulty, as well as by root cause. If the Application has been assessed previously by Verizon, a trend analysis will be included, with a graphic of progress in securing the mobile applications. The results and security posture of the mobile applications are analyzed, with recommendations for remediation of vulnerabilities, policy, procedures and governance by Customer.

3. **Documentation to be produced by Customer and Customer Obligations (if any).** Delivery of the Professional Services by Verizon is dependent on Customer's performance of the following tasks:

3.1 Customer will appoint a single point of contact / program management team for co-ordination of the Project activities for interaction with Verizon and ensuring smooth data flow and exchange of information required for execution of the Project within the agreed time-frame.
3.2 Customer will provide the necessary credentials and profiles to Customer's VPN and applications during (or prior to) the kickoff meeting.
3.3 Customer will provide and confirm that the IP addresses and subnets within the scope of work are allocated to the Customer, and that any required authorization to perform the testing has been obtained.
3.4 Customer will be responsible for providing a facility with work stations and network connectivity for the Verizon provided server on the dates, times, and locations specified in the Project Plan.
3.5 Customer will provide "Whitelisting" for Verizon source subnet's during the course of the engagement within any prevention systems (intrusion prevention systems, application firewalls, etc.). This will be applied to all Customer intrusion prevention systems monitoring all network paths to the systems to be tested, before the testing begins, and will be removed once testing is completed.
3.6 Customer will notify Verizon of any exclusion of any specific application, devices, services, or functionality that should not be tested, during (or prior to) the kickoff meeting.
3.7 Customer will configure any wireless network(s) to be tested in a test or development environment in an environment with duplicate functionality of Customer's production environment.
3.8 Customer will not make any changes to the wireless network(s) being assessed during the Project. If changes to the wireless networks are necessary and affect the application or its environment, then Verizon will be notified in advance by Customer.

4. **Assumptions (if any).** Delivery of the Professional Services by Verizon is predicated on the following assumptions and conditions:
4.1 Customer retains responsibility for the implementation of any changes to wireless network(s) managed by Customer or associated service providers under this SOW.
4.2 Access to the systems, applications, and Customer contacts must be provided by Customer during designated time frames, which will be established during the Project kick-off meeting. The failure to provide this timely access could delay completion of the Professional Services.
4.3 Verizonwill utilize its own laptops with disk or volume encryption employed for any Customer data stored during the Project.