Rapid Response Retainer Professional Service Description
Internal Network Penetration Testing

1. **Scope of Work.**

1.1. **Internal Network Penetration Testing.** The Project consists of network penetration testing (the "Professional Services"). Verizon will perform a network penetration test (the "Pen Test") to identify and exploit network and host based security vulnerabilities within the Customer's internal networked infrastructures. Verizon will prioritize systems that Customer has identified as a priority. The Pen Test consists of the following phases:

1.1.1. **Active Host Identification (Device Discovery).** Verizon will establish a profile of Customer-provided internal accessible internet protocol ("IP") subnets to identify the active devices defined in the Engagement Letter (the "Devices") within those subnets.

1.1.2. **Vulnerability Scanning.** Verizon will analyze available network services and the IP stack fingerprints of active Devices identified.

1.1.3. **Vulnerability Validation.** Verizon will validate the results of vulnerability scanning in order to identify (and disregard) false-positive results and validate other positive results from automated testing.

1.1.4. **Exploitation.** Once Verizon establishes an understanding of Device roles, potential trust relationships, accessible network services and potential vulnerabilities, Verizon will attempt to gain access to target systems.

1.1.5. **Post-Exploitation.** Once Verizon completes exploitation and if it has achieved access to any vulnerable hosts and data, Verizon will attempt to escalate privileges on these exploited host(s). Verizon will attempt to leverage this access and access to data (such as password hashes and authentication tokens) on these hosts to gain additional access into the Customers network (as applicable and within scope) and attempt to access additional systems and data.

1.1.6. **Basic Sensitive Data Discovery.** In order to identify Sensitive Data (as defined below) that may be at risk of compromise, Verizon will attempt to gain administrator-level access and search the local file systems of exploited Devices for Sensitive Data. The Sensitive Data discovery has two components:

1.1.6.1. **Manual component.** Verizon consultants will manually search the file systems for Sensitive Data.

1.1.6.2. **Automated component**: Verizon will use automated tools, including proprietary Verizon tools such as OpenDLP, to search the file systems for Sensitive Data.

1.1.6.3. "Sensitive Data" consists of:

- Credit card numbers;
- Credit card track data;
- Social security numbers;
- Payroll data; and
- Other Customer information, subject to mutual agreement.

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; and

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 (i) Customer's Devices and (ii) each Device's associated unauthenticated applications, as well as recommended remediation steps. Screen shots and log excerpts may be included, if applicable.

2.2.1. The Report will include an "Executive Summary," which will contain 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 a Device has been assessed

previously by Verizon, a trend analysis will be included, with a graphic of progress in securing the network. The Report will also include recommendations for remediation of vulnerabilities by Customer.

2.2.2. The contents of the Report will also be reviewed with Customer remotely via telephone.

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 Devices 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 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.

3.5. 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. Customer will provide any access to the Device(s) to be tested that may be required by Verizon.

3.6. Customer will configure any Devices to be tested in a test or development environment in an environment with duplicate functionality of Customer's production environment.

3.7. Customer will not make any changes to the Device(s) being assessed during the Project. If changes to the Devices are necessary and affect the Device 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 applications or devices 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. Verizon will utilize its own laptops with disk or volume encryption employed for any Customer data stored during the Project.

4.4. The Professional Services will be performed remotely by Verizon, unless otherwise agreed.