Rapid Response Retainer Professional Service Description
Application Vulnerability Assessment

1. **Scope of Work.**

1.1 **Application Vulnerability Assessment.** Verizon will perform an "Application Vulnerability Assessment" to identify vulnerabilities in applications residing on Customer's networked systems that offer user or inter-process interfaces, such as web applications and "thick" clients. With Application Vulnerability Assessment, Verizon will examine Customer's application's components and technologies to identify vulnerabilities in systems, server systems, static content, and server-side programs that implement the application logic.

1.1.1 Verizon will identify common and more unique application flaws. Verizon will test for common application flaws, such as stack overflows and format string issues. In addition, Verizon will examine the application's underlying design for unique vulnerabilities that may not be easily recognizable during a more superficial investigation.

1.1.2 Verizon will perform checks based on industry-specific guidance, industry practices, and standards. As determined necessary by Verizon, application components will be tested for improper configuration, session tracking weaknesses, encryption implementation and strength, input validation, flaws in server-side executables, and sensitive or unnecessary information within HTML content.

1.1.3 Verizon will perform application security testing of the Customer's applications through automated web application scanning as well as manual application functionality testing. Verizon's testing techniques include the following:

1.1.3.1 Input validation bypass. Verizon will remove client side validation routines and bounds-checking restrictions to confirm controls are implemented on application parameters sent to the server.

1.1.3.2 SQL injection. Verizon will submit specially crafted SQL commands in input fields to validate input controls are in place for the protection of database data.

1.1.3.3 Cross-site scripting. Verizon will submit active content to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test validates user input controls.

1.1.3.4 Parameter tampering. Verizon will modify query strings, parameters, and hidden fields in an attempt to gain unauthorized access to user data or application functionality.

1.1.3.5 Cookie poisoning. Verizon will modify data sent in cookies in order to test application response to receiving unexpected cookie values.

1.1.3.6 User privilege escalation. Verizon will attempt to gain unauthorized access to administrator or other users' privileges.

1.1.3.7 Credential manipulation. Verizon will modify identification and authorization credentials in an attempt to gain unauthorized access to other users' data and application functionality.

1.1.3.8 Forceful browsing. Verizon will enumerate files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.

1.1.3.9 Backdoors and debug options. Verizon will identify code left by developers for debugging purposes that could potentially allow an intruder to gain additional levels of access.

1.1.3.10 Configuration subversion. Verizon will assess Customer's web servers and application servers for improper configurations that could create attack vectors.

1.1.3.11 Test environments. Some Applications (as defined below) to be tested will be in a Customer test or development environment.

1.1.4 Verizon will perform the Application Vulnerability Assessment for the applications listed in the Engagement Letter (the "Applications"). The Professional Services will be provided performed remotely by Verizon, unless otherwise agreed.

1.1.5 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.** 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 vulnerabilities identified by Verizon in order of severity (the "Report"). 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.

      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 an Application 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.** 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.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 Application(s) to be tested that may be required by Verizon.

   3.6 Customer will configure any Applications 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 Application(s) being assessed during the Project. If changes to the Application(s) 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 applications or devices managed by Customer or associated service providers under the Project.

   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.