Rapid Response Retainer Professional Service Description
Cyber Incident Capability Assessment

The following cyber incident capability assessments are available as described in Customer's SOW;

1. Executive Breach Simulation;
2. First Responders Training Course;
3. Incident Response Readiness Assessment; or
4. Network Health Checks.

1. Executive Breach Simulation

1.1 Scope of Work

1.1.1 **Executive Breach Simulation.** Verizon will conduct an executive breach simulation (the "Simulation") as a mock incident response exercise for Customer's senior executives. The objective of the Simulation is to evaluate Customer's existing processes and procedures for responding in real time to a computer security emergency.

1.1.1.1 The Simulation will be based on a mock security emergency scenario agreed by Verizon and Customer in advance, but not known to Customer's Simulation participants (the "Scenario"). Verizon will moderate the Simulation by introducing the Scenario and prompting Customer participants for feedback and participation relative to their respective areas of organizational responsibility. Verizon will then lead the Customer participants through the Scenario.

1.1.1.2 In advance of the Simulation, Verizon will work with a maximum of two Customer personnel ("Trusted Agents") to define the Scenario and the objectives, stages and duration of the Simulation. Subject to mutual agreement, the Scenario may address Customer's potential cyber security issues, which may include elements of a wide variety of cyber security incidents, including unauthorized access, malicious code, inappropriate use or abuse, phishing and social engineering, theft of sensitive data, and point-of-sale device compromise.

1.1.1.3 This service will be delivered during one (1) business day, and run for up to a four (4) hour period. Upon completion of the Simulation, Verizon will provide a report of observations and recommendations (the "Executive Breach Simulation Report").

1.2 **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:

1.1.2 Executive Breach Simulation Report

2. First Responders Training CourseScope of Work

2.1.1 First Responders Training Course. Verizon will provide training to Customer's first responders and/or members of Customer's incident response team ("Attendees"). Training focuses on basic skills and industry practices for first responders. Training modules includes topics such as proper evidence handling and chain of custody issues, collecting and preserving data of evidentiary value, including volatile data and forensic imaging techniques, and basic forensic analysis techniques.

2.1.1.1 Verizon will provide up to two (2) instructors to perform one (1) training course which will take place in two (2) days (maximum of sixteen (16) hours onsite) for up to twenty (20) Attendees. Topics included in the 2-day First Responder's training course include the following:

- Current security trends and incident response case studies;
- Incident response process;
- Evidence handling procedures;
- Volatile data collection and tactical analysis techniques;
- Forensic imaging techniques;
- Basic forensic analysis techniques – system analysis; and
- Mock incident table-top exercise.

2.1.1.2 Additional training topics may be offered on a case by case basis as shown in the Engagement Letter. The training course will be conducted during Verizon's normal business hours at a Customer Site and on a date mutually agreed to and detailed in the Engagement Letter.

2.1.1.3 Verizon will provide training materials ("Training Materials") and a certificate of training to Attendees.

2.2 **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:

2.2.1 Training Materials

3. **Incident Response Readiness Assessment**

3.1 **Scope of Work**

3.1.1 Incident Response Readiness Assessment. Verizon will review Customer's existing incident response capability, systems, platforms, data stores, and conduct a review of Customer's existing incident response policies and processes, tools, training, and testing initiatives to gain an understanding of the Customer's network infrastructure, electronic asset inventory, and threat profile. This Assessment may include:

- A review of Customer's existing incident response plan documentation, including written incident response policies and procedures;
- An interview of key incident response stakeholders to determine roles, responsibilities, and process within Customer's incident response plan;
- A review of relevant tools, platforms, technologies leveraged by Customer for incident response purposes; and
- Verizon will provide a report of recommendations and observations (the "Incident Response Assessment Report").

3.2 **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**:**

3.2.1 Incident Response Assessment Report

4. **Network Health Checks**

4.1 **Scope of Work**

4.1.1 Network Health Checks. Verizon will capture and analyze 14 consecutive days of netflows stemming from Customer IP address ranges listed in the Customer IP ("CIP") schedule provided by Customer as requested by Verizon (the "CIP Schedule"). Verizon will analyze those traffic patterns matching Customer's identified CIP addresses against the Verizon watchlist. The watchlist contains IP addresses deemed suspect by Verizon based on the collection and scrutiny of intelligence drawn from the Verizon global IP backbone, investigations, and other sources. Verizon will match watchlist IP addresses against Customer inbound and outbound traffic to identify possible indications of unwanted activity.

4.1.1.1 Verizon will examine the metadata (e.g., source and destination IP addresses, source and destination ports, packet count and bytes) in Customer's inbound and outbound communications to search for known threat actors, as well as traffic patterns that are considered malicious. Verizon will supplement the netflow health check by IP-heavy firewall logs Customer has obtained through Customer's security event management tool and provided to Verizon for analysis.

4.1.1.2 Verizon will provide Customer with a report of findings and recommendations (the "Network Health Check Report"). The Network Health Check Report will provide a brief executive summary, as well as details on the presence of potentially malicious, unauthorized, or unwanted activity, if any. Verizon will also provide recommendations related to the findings. The Network Health Check Report will explain Customer's strengths and weaknesses, and identify areas that can be improved.

4.2 **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:

4.2.1 Network Health Check Report