Appendix E Services Description and Engagement Letter Template

DIR-CPO-4889

This attachment includes service descriptions for the following Verizon Technical Services offerings:

Rapid Response Retainer Service Descriptions

This section includes the following Rapid Response Retainer Service Descriptions (SOWs associated with each Service element):

- **Rapid Response Retainer SOW – General Service Description (including Core Package)**
- **Rapid Response Retainer Cyber Incident Capability Assessment Options**
  - Executive Breach Simulation
  - Cybersecurity First Responder's Training
  - Incident Response Plan Assessment
  - Network Health Check
- **Rapid Response Retainer Optional Add-Ons**
  - Network Telemetry Analysis
  - Dark Web Hunting
  - Endpoint Telemetry Analysis
  - Backbone NetFlow Collection
- **Rapid Response Retainer Security Technical Advisory Options**
  - Governance, Risk and Compliance
  - Payment Card Industry
  - Threat and Vulnerability Management
    - Application Vulnerability Assessment
    - Internal Network Penetration Testing
    - Wireless Vulnerability Assessment
  - Risk Services
    - Attack Detection Assessment
    - Incident Response Capability Assessment
    - Emergency Services
    - Espionage Health Check
    - Incident Analytics
    - Malcode Analysis
    - Retail Health Check
- **Forms**
  - Engagement Letter
  - Customer IP Address Schedule

RAPID RESPONSE RETAINER GENERAL SERVICE DESCRIPTION - INCLUDING CORE PACKAGE

TECHNICAL SERVICES RAPID RESPONSE RETAINER STATEMENT OF WORK TO VERIZON TECHNICAL 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 (SOF). This SOW is subject to DIR Contract DIR-CPO-4889 (the "DIR Contract"). In the event of a conflict between this SOW and the DIR Contract, the DIR Contract shall control.

1. PROJECT DESCRIPTION

1.1 **General Scope of Work.** Verizon's Rapid Response Retainer service helps prepare for, reduce the response time of, reduce the impact of, and respond more effectively to a cybersecurity incident. The core of the Rapid Response Retainer provides response capabilities, including retained hours to use on assessments, health checks or incident response planning. The Rapid Response Retainer core service can be enhanced with Add-on capabilities which provide investigators with tools and means for even more effective and immediate access to data when an incident occurs. Verizon will provide Customer with the Rapid Response Retainer core services, and any of the Add-on capabilities indicated on the SOF.

1.2 **Rapid Response Retainer – Core Service.** The Rapid Response Retainer core service includes certain activities that utilize security technical advisory support hours (Hours) as requested by Customer using the Engagement Letter process, each described below.

1.2.1 **Onboarding.** Within 10 days of the commencement of a Service Commitment, Verizon will send an email to Customer's point of contact (POC) requesting a date and time for a Rapid Response Retainer onboarding discussion. Onboarding will take place either in person, or via a conference call between Customer and Verizon. During the Onboarding session, Verizon will: (i) collect Customer contact information, (ii) collect the list of countries where Customer may need Services (as provided in the Project Delivery Countries section below) (the Country List); and (iii) collect any information required from Customer for registration into the Services which will include information required by any core services or Add-on capabilities ordered. Onboarding also includes:

- Review of Service components and the Engagement Letter process for requesting Services for a Project.
- Name of the Verizon designated investigative liaison contact, each as further described below.
- Escalation processes for Emergency Services.
- Customer selection of one Cyber Incident Capability Assessment (Annual Assessment) per twelve month period during the Service Commitment from the four available Annual Assessment options and requested schedule for delivery of the Annual Assessment. Verizon and Customer will agree on a time and location for the Annual Assessment. Following Onboarding, Verizon will forward Customer an Engagement Letter for Customer's execution containing the name of the Annual Assessment selected and agreed upon schedule.
- Network Sensor(s) deployment instructions.

Once the Onboarding process is complete, Customer will be able to order additional Services in addition to the Annual Assessment via the Project initiation process described below.

1.2.2 **Security Technical Advisory Support.** Following Onboarding, Customer may order any of the Services described in this SOW. The ordered Services will be provided with the number of Hours stated in an Engagement Letter. Pre-purchased Hours must be used during the Service Commitment and will expire at the end of the Service Commitment term. The hourly rates for the Hours are shown in the SOF.

***Verizon has also provided Services descriptions and related documents in this Appendix E.*

1.2.3 **Project Initiation Process (Engagement Letters).** After the Onboarding process is complete, when Customer wishes to request additional Services, Customer will contact the Verizon by calling the Hotline, and initiate the Service via an Engagement Letter. The scope of each Engagement Letter will be agreed upon on a case-by-case basis. When Customer orders a Project, Verizon will provide an Engagement Letter that describes the Project requested, methodologies to be used in performance of the requested Project, the hourly rate to be used from the Customer SOF, and for non-Emergency Services, the number of Hours required to complete the requested Project that is developed on a call with Customer. All Engagement Letters will be in writing. Customer must sign the Engagement Letter prior to any Project being performed. The signed Engagement Letter will become part of the Customer Service Agreement. Any changes to an Engagement Letter require an amended and executed Engagement Letter. In the event of a conflict between the terms and conditions of the Agreement, the order of precedence shall be: the SOF, the Master Terms, the PSA, the SOW, and then the Engagement Letter.

1.2.4 **Cyber Incident Capability Assessments.** An Engagement Letter is required for an Annual Assessment. Rapid Response Retainer core service includes a choice of one of the Annual Assessments listed below, to be delivered during each twelve month period (Contract Year) of the Service Commitment, which Customer may choose during the Onboarding session or during subsequent discussions, as part of the Rapid Response Retainer core service. Customer may choose additional assessments using Hours as required by such assessment. If Customer does not want one of the four available Annual Assessments as part of the core service, Customer may request an alternate Service (as offered pursuant to this SOW), equivalent to no more than 40 Hours of support. The Annual Assessment choice is available for selection during the relevant Contract Year and must be ordered by Customer within 90 days of the end of the Service Commitment term. Annual Assessments expire at the end of the Service Commitment term. The Annual Assessment may be rescheduled or delayed for Emergency Services. The Engagement Letter will describe the specific scope and Deliverables for each of the Annual Assessment options below.

- Executive Breach Simulation;
- Cybersecurity First Responders Training Course;
- Incident Response Plan Assessment; or
- Network Health Checks.

1.2.5 **Network Sensors.** Verizon will work with Customer to deploy up to two lightweight software sensors (Network Sensors) in Customer's environment. These Network Sensors can be deployed on existing Customer hardware or as a virtual machine that is running a supported

Linux-based operating system. Verizon does not supply hardware as part of this service. The Network Sensors are configurable to enable Verizon to collect, filter, and analyze network data. During Onboarding, Verizon will work with Customer to select the areas where the Network Sensor(s) will be deployed in the Customer environment and will be configured to capture a set amount of traffic based on the company size, after which the Network Sensors will be put into a passive mode until required for use during an Project pursuant to an Engagement Letter. Additional support beyond reasonable installation and maintenance of the deployed instances of the Network Sensor(s) on Customer's network may require the use of Hours, which can be ordered pursuant to an Engagement Letter at the hourly rate identified in the SOF (rate for VTRAC Services). In the event Verizon is engaged to provide Emergency Services, Verizon will leverage network data captured by the Network Sensor(s) to perform deep packet inspection locally, applying a capture policy to the traffic, and then encrypting, compressing and streaming it back to the Verizon's cloud platform for analysis. The Verizon cloud platform does not perform SSL (Secure Sockets Layer) decryption. Network Sensors capture network packet data transmitted on a network with no encryption. Customer may also request Verizon conduct unique, periodic, or one-off analysis leveraging the Network Sensor(s). Scope and pricing for analysis requests will be outlined in an Engagement Letter and provided pursuant to the hourly rates identified in the SOF (rate for VTRAC Services).

1.2.6 **Incident Response Hotline Access.** Verizon will provide a toll-free telephonic support number that is available 24x7x365 (Hotline). The Hotline is to be used by Customer when Customer has a security incident and requires Rapid Response Retainer support. Upon calling the Hotline, a Verizon representative will log the Customer's information and reason for the call, and will engage the next level of phone support.

1.2.7 **Investigative Team Phone Support / Remote Support.** When Customer calls the Hotline, with a suspected security incident, a member of Verizon's investigative team will return the Customer's call within the three hour SLA to get more information related to the security incident. If the call requires a Project to be initiated, the investigative response team member will define the scope of the Project in an Engagement Letter and schedule the Project for delivery as required.

1.2.8 **Investigative Liaison.** Verizon will provide an investigative liaison (Liaison) who will provide Customer with a consistent interface to Verizon's investigative response team. The Liaison will serve as a contact point for non-emergency response questions or issues regarding the Rapid Response Retainer service, and in some cases may directly contribute to the delivery of Services for Customer's reactive emergency response and proactive incident response technical advisory engagements.

1.2.9 **Intelligence Summaries.** Verizon will email Customer POCs with Verizon's research, investigations, solutions, and knowledge intelligence, which may include communications, such as weekly intelligence summaries and monthly intelligence briefings (phone and web conference).

1.2.10 **Project Management.** Verizon will be responsible for managing the Project change control process. Should the Project's requirements change during the course of a Project, Verizon will ensure that any modifications to scope, budgeted number of Hours and schedule are appropriately documented in an amended Engagement Letter.

1.3 **Rapid Response Retainer – Emergency Services**

1.3.1 **Emergency Services.** An Engagement Letter is required for Emergency Services and uses Hours as applicable.

1.3.1.1 **On Site Response with In-Transit SLA.** When the Parties agree that a member of Verizon's investigative response team must travel to a Customer Site, the Verizon investigative response team member will be "in-transit" to the Customer Site within 24 hours of (a) Customer's execution of the Engagement Letter and (b) Verizon's procurement of all required travel documentation and Customer's approval if required. "In-transit" means the investigative response team member is traveling to the Customer Site. The in-transit SLA clock begins when (a) and (b) are both complete and stops when the investigative response team member is in-transit. Verizon's investigative response phone support is available while the investigative response team member is in-transit.

1.3.1.2 **Emergency Services Phases.** Emergency Services are provided in 2 phases, Incident Response and Forensic Analysis. Customer and Verizon will determine which of the phases are required for an Emergency Services Project.

1.3.2 **Malcode Analysis.** An Engagement Letter is required for Malcode Analysis and uses Hours as applicable. Malcode Analysis provides analysis of files that Customer suspects might be malicious..

1.3.2.1 **Malcode Analysis SLA.** Within 24 hours of receipt of a signed Engagement Letter and Customer's suspect files received at the Verizon server, Verizon will perform an analysis of the files and provide Customer with the Malcode Analysis Report. If additional analysis is required after the first 24 hours, Verizon will continue with the service as described in the Engagement Letter.

1.4 **Rapid Response Retainer – Add-on Capability.** As an enhancement to the Rapid Response Retainer core services, Customer may order any of the following Add-on capabilities in the SOF.

- Network Telemetry Analysis;
- Dark Web Hunting;
- Endpoint Telemetry Analysis;
- Backbone NetFlow Collection.

2. **SUPPLEMENTAL TERMS**

2.1 **Service Commitment.** The Service Commitment is for a 12 month term, 24 month term, or, 36 month term, as identified on the SOF.

2.2 **Service Level Agreement Terms.** The Services listed below have SLAs. If Verizon fails to meet the respective SLA, Customer's remedy shall be a credit of an additional five Hours of security technical advisory support, which may be used within Service Commitment term. An SLA remedy will be documented in an Engagement Letter showing the increase in the Hours at no additional cost to Customer. The SLAs are described above for the following Services:

- Investigative Team Phone Support / Remote Support;
- Emergency Services On Site In-Transit SLA;
- Malcode Analysis SLA.

2.2.1 **SLA Conditions.** The following conditions apply to SLAs:

- No SLA remedy will be due to the extent the SLA is not met because of any act or omission

on the part of Customer, its contractors or vendors, or any other entity over which Customer exercises control or has the right to exercise control.

- No SLA remedy will be due to the extent the SLA is not met because of a Force Majeure Event, as defined in the DIR Contract.
- No SLA remedy will be due to the extent the SLA is not met because of the amount of time delays caused by incorrect or incomplete information provided by Customer.

2.3 Customer Obligations

2.3.1 **Customer IP Consents, Representations and Warranties.** Customer consents to Verizon's scanning and monitoring of Customer IP (CIP) and associated network components, the collection, use, processing, analysis and disclosure to Customer POCs Customer's Internet traffic data, and the use of threat intelligence pertaining to CIP in an aggregated and anonymized form with Verizon's portfolio of security services. Customer represents and warrants that: (i) the Customer provided list of CIP addresses contains only IP addresses assigned or allocated for the exclusive use of Customer and/or Customer Affiliates over which Customer has control; and (ii) Customer has all legally required consents/permissions from CIP users for Verizon's performance of the Service. For Services that include a network sensor, Customer understands that the network sensor will collect, analyze and provide reporting on data packets, traversing Customer's network to which such network sensor is attached.

2.3.2 **Project Delivery Countries.** Verizon will only perform Services in the countries listed in the Country List provided by Customer during initial Onboarding.

2.3.3 **[RESERVED]**

2.3.4 **Customer Notices.** Unless otherwise required (e.g., by Payment Card Industry requirements), Customer is responsible for the collection and dissemination of all information regarding an incident and Rapid Response Retainer service does not include nor provide notification services.

2.3.5 **Payment Card Industry Project.** If a Service involves data that is subject to the Payment Card Industry (PCI) Security Standards Council (the PCI Council) requirements, Verizon shall have the right to disclose the results of the Services (including any report of compliance, working papers, notes and other information) to the PCI Council and other parties as required under the PCI Forensic Investigator (PFI) Program Guide and the qualified security assessor (QSA) Validation Requirements (Supplement for PCI Forensic Investigators) promulgated by the PCI Council. Copies of the PCI Council's current standard PCI Forensic Investigator Program Guide and QSA Validation Requirements (Supplement for PCI Forensic Investigators) are available on the PCI Council's website (see www.pcisecuritystandards.org).

2.3.6 **Recommendations.** Customer is responsible for the decision to implement (or not to implement) any recommendations. Verizon is not responsible for the results achieved from any Customer implementation.

3. FINANCIAL TERMS

3.1. **Rates and Charges.** Subject to the DIR Contract, Customer will pay an annual recurring charge as set forth in the SOF. Travel and expenses will be billed as provided in the PSSA, this SOW, and the SOF.

3.2. **Project Charges.** Subject to the DIR Contract, for additional Projects or Services provisioned under this SOW, Customer will be invoiced on a time and material basis at the rate identified on the Engagement Letter, and at the rates listed in the SOF.

RAPID RESPONSE RETAINER CYBER INCIDENT CAPABILITY ASSESSMENT

Pursuant to Section 1.2.4 above, an Annual Assessment Rapid Response Retainer core service includes a choice of one of the Annual Assessments listed below. The descriptions follow:

- Executive Breach Simulation;
- Cybersecurity First Responders Training Course;
- Incident Response Plan Assessment; or
- Network Health Checks.

Rapid Response Retainer Technical Service Description
Cyber Incident Capability Assessment: Executive Breach Simulation

This service description describes the Executive Breach Simulation (Simulation), which may be selected as the Customer's annual Cyber Incident Capability Assessment choice included in the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work). An Engagement Letter will describe the specific scope and Deliverables for the assessment described below.

1. **SERVICE DESCRIPTION.** Following signature on an Engagement Letter, Verizon will conduct a kick-off call to discuss resources, confirm the trusted agents and Simulation attendees, date location and agenda for the Simulation, and confirm other details contained in the Engagement Letter. The objective of the Simulation is to evaluate Customer's existing processes and procedures for responding in real time to a computer security emergency. The Simulation will be based on a mock security emergency scenario agreed by Verizon and Customer in advance (the "Scenario," as further defined below), but not known in advance by Customer's Simulation participants. 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. In advance of the Simulation exercise, Verizon will work closely with one to two Customer personnel ("Trusted Agents") to define the Scenario and the objectives, stages and duration of the Simulation. The Simulation exercise will be performed at a Customer location, as further identified in the Engagement Letter. The duration for the Executive Breach Simulation shall be one business day and run for up to a four hour period, unless otherwise agreed in writing by the Parties.

2. **DELIVERABLES AND DOCUMENTATION.** Upon completion of the Simulation, Verizon will provide a report of observations and recommendations.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - The Services are based on Verizon's understanding of Customer's requirements. Should the scope of the Project change, Verizon will continue to work only after mutual execution of an amended Engagement Letter.
   - Customer must provide an overhead projector and compatible overhead projector screens on which to display the overhead projector material.
   - Customer must identify in advance the Trusted Agents, who will work with Verizon to define the Scenario and develop the stages, discussion points, and duration of the Simulation.
   - Customer must assure the participation during the Simulation of senior executive staff from each of the Customer's functional organizations with a role within Customer's computer emergency management processes and procedures.
   - At or before the kick-off call, Customer shall provide appropriate on-site authorization documentation (where applicable).

Rapid Response Retainer Technical Service Description
Cyber Incident Capability Assessment: Cybersecurity First Responder's Training

This service description describes the Cybersecurity First Responder's Training (Training), which may be selected as the Customer's annual Cyber Incident Capability Assessment choice included in the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work). An Engagement Letter will describe the specific scope and Deliverables for the assessment described below.

1. **SERVICE DESCRIPTION.** Following signature on an Engagement Letter, Verizon will designate a point of contact for the Training, who will develop and provide a Training agenda (Training Agenda), and conduct a kick-off call to discuss resources and confirm details contained on the Engagement Letter. Delivery of the Training will include up to two Verizon instructors who will provide a two-day Training to Customer's cybersecurity and incident response employees (Attendees). The Training incorporates industry practices and standards for responding to, and investigating cybersecurity incidents and data security breaches, and leverages real-world cybersecurity incident and data breach scenarios experienced by the Verizon Threat Research Advisory Center team (VTRAC). The Training will focus on the practical application of tasks and techniques commonly encountered during cybersecurity incidents, and will include the following topics:
   - Incident Response Concepts and Preparations;
   - Windows Memory Dump Acquisition;
   - Windows Volatile Data Capture and Analysis;
   - Windows Live System Auditing;
   - Windows Full Disk Imaging;
   - Windows File Collection and Tactical Timelining;
   - Windows Memory Dump Parsing and Analysis;
   - Windows File System Artifact Parsing and Analysis.

   After the Training, Verizon will provide Customer with a PDF version of the Power Point presented in Training (Training Materials).

2. **DELIVERABLES AND DOCUMENTATION.** Any Deliverables provided by Verizon will be identified in the engagement letter. Verizon will provide:
   - Training Agenda; and
   - Training Materials.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - The Services are based on Verizon's understanding of Customer's requirements. Should the scope of the Project change, Verizon will continue to work only after mutual execution of an amended Engagement Letter.
   - Each Attendee will bring a laptop to the course, or will use a computer provided by Customer in Customer's training facility.
   - Each course will have a maximum of twenty Attendees.
   - As requested by Verizon, Customer will download the requisite tools from the internet to Attendees' computers prior to the start of the course.

Rapid Response Retainer Technical Service Description
Cyber Incident Capability Assessment: Incident Response Plan Assessment

This service description describes the Incident Response Plan Assessment (IR Plan Assessment), which may be selected as the Customer's annual Cyber Incident Capability Assessment choice included in the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work). An Engagement Letter will describe the specific scope and Deliverables for the assessment option described below.

1. **SERVICE DESCRIPTION.** Following signature on an Engagement Letter, Verizon will conduct a kick-off call to discuss resources, and confirm details contained in the Engagement Letter. Verizon's IR Plan Assessment will review and assess Customer's current policies, processes and procedures, documented within Customer's existing IR plan, related to Customer's IR program. Verizon will focus the IR Plan Assessment on the activities surrounding cybersecurity alerts and events that meet the threshold required to invoke Customer's IR processes. The IR Plan Assessment will be delivered in two phases as described below:

1.1 **Phase 1: Review Customer's IR Documentation.** During phase 1, Verizon will review Customer's documented policies, procedures, work flows, and any other documentation related to Customer's IR plan (Plan). Verizon will review the Plan against generally accepted industry practices for incident response. The information that will be included in the IR Plan Assessment will be grouped into the following six categories:

- Planning and preparation;
- Detection and classification;
- Collection and analysis;
- Containment and eradication;
- Remediation and recovery; and
- Assessment and reporting.

The purpose of the review will be to identify gaps in Customer's existing IR Plan, such as roles and responsibilities of IR stakeholders, escalation and communication processes, incident handling coordination measures, and other functions critical to executing an IR process.

1.2 **Phase 2: Review Customer's IR Tools and Environment.** During phase 2, Verizon will work with Customer to identify hardware and software tools, systems, and platforms (collectively IR Tools) leveraged by Customer for IR purposes, relative to the six categories of the IR process referenced above. Verizon will work with Customer to identify gaps in Customer's IR Tools and determine their suitability for IR, investigative and incident management purposes.

1.3 **Report.** Upon completion of Phase 1 and Phase 2, Verizon will produce a "Management Report" which will include observations from both phases and provide recommendations designed to enhance, mature, or improve Customer's IR capabilities. The Management Report may, at Customer's request, including a recommendation for training course(s) for Customer's security personnel.

2. **DELIVERABLES AND DOCUMENTATION.** Any Deliverables provided by Verizon will be identified in the engagement letter. Verizon will provide Management Report and deliverables as described in an Engagement Letter.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - The Services are based on Verizon's understanding of Customer's requirements. Should the scope of the Project change, Verizon will continue to work only after mutual execution of an amended Engagement Letter.

Rapid Response Retainer Technical Service Description
Cyber Incident Capability Assessment: Network Health Check

This service description describes the Cybersecurity Network Health Check (Health Check), which may be selected as the Customer's annual Cyber Incident Capability Assessment choice included in the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work). An Engagement Letter will describe the specific scope and Deliverables for the assessment described below.

1. **SERVICE DESCRIPTION.** Following signature on an Engagement Letter, Verizon will conduct a kick-off call to discuss resources, and confirm details contained in the Engagement Letter. Customer will provide Customer IP address ranges on a signed Customer IP schedule (CIP Schedule). After receipt of the CIP Schedule, Verizon will begin to capture and analyze 14 consecutive days of netflows stemming from Customer IP address ranges listed on the CIP Schedule. Verizon will analyze those traffic patterns matching Customer's identified CIP addresses against the Verizon watchlist. The Verizon 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. 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.

2. **DELIVERABLES AND DOCUMENTATION.** Any Deliverables provided by Verizon will be identified in the engagement letter. Verizon will provide Customer with a report of findings and recommendations ("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.

3. **CONDITIONS.** Customer must provide a fully completed and executed CIP Schedule.

*RAPID RESPONSE RETAINER OPTIONAL ADD-ONS

As an enhancement to the Rapid Response Retainer core services, Customer may order any of the following Add-on capabilities. Each Add-on capability is described below.

- Network Telemetry Analysis
- Dark Web Hunting
- Endpoint Telemetry Analysis
- Backbone NetFlow Collection

Rapid Response Retainer Technical Service Description
Add-on Capability: Network Telemetry Analysis

This service description describes Network Telemetry Analysis, which may be selected as an Add-on Capability pursuant to the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work), and included in a SOF.

1. **SERVICE DESCRIPTION.** Verizon will leverage tools that provide network threat detection, and full-packet forensics for enterprise, cloud, or industrial environments. The Network Telemetry Analysis tool enables retention of network packet data (Network Data) which can be analyzed using various detection techniques, including threat intelligence, signatures, and behavioral/anomaly classifiers. Network Data may include any technical data and related information about the Customer environment, including, but not limited to the operating system type and version; network host data; origin and nature of malware, endpoint GUID's (globally unique identifiers); Internet Protocol (IP) addresses; MAC addresses; log files; network configurations; network security policies; information related to the usage, origin of use, traffic patterns, and behavior of the users on a network; and any aggregate, demographic or network traffic data. Verizon will leverage Network Sensors installed locally on a Customer's network or cloud environment to passively capture Network Data and stream to the Verizon platform for analysis, threat detection, and correlation of threats, and to create a forensic memory of the Network Data for a thirty day retention period. Verizon will use this tool to have visibility into Network Data for impact analysis, investigation, and response. The Network Telemetry Analysis Add-on, is available in four sizes, and Customer will order the annual license coverage option, based on the number of employees in the Customer's company, as detailed on the SOF. Size options for license coverage include:
   - Option 1: Up to 2,500 employees (includes 2 sensors) / Up to 25 Mbps of network traffic;
   - Option 2: 2,501- 10,000 employees (includes 2 sensors) / Up to 50 Mbps of network traffic;
   - Option 3: 10,001-50,000 employees (includes 2 sensors) / Up to 100 Mbps of network traffic; or
   - Option 4: 50,001+ employees (includes 2 sensors) / Up to 500 Mbps of network traffic.

1.1 **Services.** When ordered as an Add-on capability to the Rapid Response Retainer, Network Telemetry Analysis will allow Verizon to perform the following services:

1.1.1 **Monthly Analysis.** Leveraging Customer's network traffic collected by the deployed Network Sensors, Verizon will conduct a monthly analysis of the captured packet data. Verizon's analysis will include high level operational and security observations designed to help Customer be more attuned to the organization's security posture, and identify potential C2 (command and control) communications, indicators of compromise, and other suspicious or potentially malicious activity. After performing the analysis, Verizon will email the Customer a written report of findings. Verizon will promptly report critical findings via the communication method established during Rapid Response Retainer Onboarding. All monthly analysis activities will be performed during Business Hours and on a schedule agreed to by Verizon and Customer.

1.1.2 **Reactive Analysis.** In the event Verizon is engaged pursuant to the Rapid Response Retainer to provide Emergency Services, Verizon will leverage Network Data captured by the Network Sensor, to perform deep packet inspection locally, applying a capture policy to the traffic, and then encrypting, compressing and streaming it back to the Verizon's cloud platform for analysis. If necessary, Verizon will work with Customer to place the Network Sensor, to update the capture profile, to capture additional data or additional network segments for up to 30 days,

enabling rapid access to full packet forensics to aid in the investigation. Additional collection of Network Data beyond 30 days will result in additional fees. The platform does not perform SSL (Secure Sockets Layer) decryption. Sensors capture network packet data transmitted on a network with no encryption.

1.1.3 **Custom Analysis.** Customer may request Verizon conduct unique, periodic, or one-off analysis (custom engagement) leveraging the deployed sensor(s). Scope and pricing for custom analysis requests will be outlined in an Engagement Letter and provided pursuant to the hourly rates identified in the Rapid Response Retainer SOF (rate for RISK Services).

1.2 **Network Sensors.** Up to two lightweight software sensors (Network Sensors) will be provided to Customer to deploy in the Customer environment. A Network Sensor is a Linux software package that captures Network Data from the Customer environment, optimizes, encrypts and transmits data back to the Verizon platform. Sensors are deployed passively off a SPAN/Tap or Mirror port from a network or tap aggregation device within the Customer environment. These sensors can be deployed on existing hardware or as a virtual machine that is running a support Linux based operating system. The Network Sensors are configurable appliances that enable Verizon to collect, filter, and analyze Network Data. Verizon will work with the Customer to select the areas that the Network Sensors will be installed in the Customer environment and will be configured to capture a set amount of traffic based on company size and package option determined on the SOF. Customer can order additional Network Sensors separately. Hardware is not included as part of this Service. Network Sensors can only be deployed in countries provided to Customer during Onboarding. Additional support beyond reasonable installation and maintenance of the deployed instances of the Network Sensor(s) on Customer's network may require additional hours, which can be ordered by an Engagement Letter at the hourly rate identified in the Rapid Response Retainer SOF (rate for RISK Services).

1.3 **Data and Data Retention.** Verizon will store collected Customer Network Data for a thirty (30) day retention period. Standard retention periods are on a rolling basis and the Customer Network Data stored is the most recently captured for the retention period selected. Customer Network Data is automatically deleted when it exceeds the thirty day data retention period.

2. **DELIVERABLES AND DOCUMENTATION.** Verizon will provide a Monthly Report and deliverables as described in an Engagement Letter.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - Customer is responsible for assisting Verizon in the deployment of the Network Sensor, by providing hardware or a virtual machine that is running a supported Linux based operating system, and ensuring Customer's local networking team is available.
   - **Interoperability.** Where applicable, Customer acknowledges that modifications or changes to the Customer environment may cause interoperability problems, inability to transmit Network Data to Verizon, or malfunctions of the Network Sensor. Customer will give Verizon written notice of any modifications or changes within five Business Days after making any such changes. Customer acknowledges that it is Customer's responsibility to maintain, at its sole cost and expense, the Customer environment to ensure that the Customer environment is interoperable with the Service.

Rapid Response Retainer Technical Service Description
Add-on Capability: Dark Web Hunting

This service description describes Dark Web Hunting, which may be selected as an Add-on capability pursuant to the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work), and included in a SOF.

1. **SERVICE DESCRIPTION.** Verizon's Dark Web Hunting service provides proactive, investigative intelligence research, analysis, and reporting to assist the Customer manage security risks and situational awareness. Verizon's Dark Web Hunting provides adversarial threat patterns and activities focused on Customer's business priorities. Dark Web Hunting includes the following:

1.1 **Keyword and Risk Areas.** Verizon will work with the Customer to determine Customer's monitoring and hunting priorities. The priorities will consist of a list of Customer keywords, and the risk areas the Customer would like Verizon to focus on during Hunting, Alerting, and Weekly Reporting. Customer keywords can encompass elements such as awareness of brand reputation, product reputation, personnel protection, physical infrastructure protection, supply chain risk management, and network architecture protection (Keywords). Verizon will search the surface, deep and dark web for Keywords identified and will focus on the risk areas that Customer identifies as its primary concern (Risk Areas). Risk Areas may include any of the following:

- Brand;
- TypoSquatting Risk;
- Domain/Sub-Domain Risk;
- IP Range Risk;
- Hash Value Risk;
- Malware Risk;
- Intellectual Property / Loss Risk;
- Third Party Risk (Includes Supply Chain/Vendors/Contractors);
- Critical Infrastructure Risk;
- Physical Security Risk;
- Human Factor Risk (C-Suite/New Hire/Separations/Insider Threat);
- Travel Risk;
- Social Engineering Risk;
- Attack Patterns;
- Vulnerability Management Risk;
- Competitor Risk;
- Fraud.

1.2 **Hunting and Analysis.** Verizon will hunt the surface, deep, and dark web of the internet for Keywords and indications of the theft or misuse of Customer information related to the Risk Areas. Verizon uses advanced open source research techniques, extensive use of numerous search engines, foreign language capabilities, forums, blogs, and dark web markets to provide detailed intelligence information produced from publicly available surface, deep and dark web information, to search for Keywords in the Risk Areas identified as priority for the Customer. Verizon will scan, and detect nefarious activity occurring outside Customer's infrastructure, to help identify and mitigate physical and cyber related adversarial activity against the Customer Risk Areas.

Verizon will collect alerts, analyze them, and then prioritize the alert by a community based risk/confidence score. A high priority finding/alert is a community based risk/confidence score of 70 or above, unless otherwise requested by Customer.

On a weekly basis Verizon will provide a weekly report including a summary of Keyword findings/alerts in the Risk Areas identified. The Weekly Reports will summarize the 15 highest priority findings based on Customer selected Keywords and Risk Areas.

1.3 **Dark Web Hunting Technical Advisory Support.** In the event Customer requires support in addition to the services above, Customer may request support from Verizon within the categories listed below. Specific services available within each category that are applicable to the Customer's needs will be discussed during a scoping call. Scope and pricing will be outlined in an Engagement Letter and will be provided pursuant to the hourly rates identified in the Rapid Response Retainer SOF (rate for RISK Services). Support categories are:

- Custom surface, deep, and dark web research;
- Custom tactical, operational, and strategic intelligence analysis; and,
- Incident response investigative activities.

2. **DELIVERABLES AND DOCUMENTATION.** Verizon will provide a Weekly Report and deliverables as described in an Engagement Letter.

3. **CONDITIONS.** Customer is solely responsible for identifying Keywords and Risk Areas.

Rapid Response Retainer Technical Service Description
Add-on Capability: Endpoint Telemetry Analysis

This service description describes Endpoint Telemetry Analysis, which may be selected as an Add-on capability pursuant to the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work), and included in a SOF.

1. **SERVICE DESCRIPTION.** Verizon will deploy an agent (provided through Tanium), on Customer's requested endpoint environment and a console an Amazon Web Services (AWS) instance in the Verizon intelligence lab for Verizon's use. Customer will not have access to the Tanium console deployed in Verizon's lab. Customer will order annual license coverage for up to 5,000 Customer endpoints, and in increments of 1,000 Customer endpoints over 5,000 as specified on the SOF. Verizon will work with Customer to gather all necessary information required to deploy the Tanium agents on Customer endpoints, and confirm whether or not Customer has purchased enough licenses to cover Customer's requested endpoint environment. When ordered as an Add-on capability to the Rapid Response Retainer, and once licenses have been enabled and Tanium agents installed and actively reporting to the Tanium console, Endpoint Telemetry Analysis will allow Verizon to commence the following services:

1.1 **Monthly Endpoint Analysis.** Leveraging the Tanium agents to retrieve data from Customer endpoints, Verizon will conduct a monthly endpoint analysis. Verizon's Monthly Endpoint Analysis will leverage the capabilities provided by the deployed Tanium modules to perform a wide variety of proactive security activities designed to help Customer gain better visibility into Customer's security posture. Examples includes: scanning networks for unmanaged assets; conducting vulnerability scans and evaluating benchmarks against standard security configurations; automating patching across the Tanium-deployed environment; searching for indicators of attacks related to threat actor tactic, techniques, and procedures; and facilitating follow-on remote investigation, quarantine and targeted remediation activities. After performing the analysis, Verizon will email the Customer a written report of findings. The Monthly Analysis activities will be performed on a schedule mutually agreed to by Verizon and Customer.

1.2 **Reactive Analysis and Response.** In the event Verizon is engaged to provide Emergency Services through an Engagement Letter process (pursuant to the SOW section 1.2.3 Project Initiation Process), Verizon can leverage the Tanium console to remotely conduct forensic investigations on suspicious machines by reviewing historical and current state data. Verizon can utilize the Tanium agents, to scope a suspected incident by performing searches of the Customer's endpoints. With Customer's consent, Verizon can also take targeted remediation actions, such as: quarantining compromised Customer machines, kill malicious processes, capture files, deploy patches, repair registry keys, apply configuration updates, uninstall applications, close unauthorized connections, and more.

1.3 **Custom Analysis.** Customer may request Verizon conduct unique, periodic, or one-off analysis (pursuant to pursuant to the SOW section 1.2.3 Project Initiation Process).

1.4 **Endpoint Telemetry Analysis SLA.** Verizon will begin remote forensic investigative support leveraging data retrieved from Customer endpoints, within six hours of receipt of a Customer signed Engagement Letter (pursuant to the SOW section 1.2.3 Project Initiation Process) requesting assistance. This SLA will only apply in the event Customer has ordered enough licenses to cover Customer's entire endpoint environment; all endpoints have Tanium agents installed, configured, and are accessible via the Tanium platform. This reduced response times

will not apply, in the event Customer has not met the requirements contained in this section.

2. **DELIVERABLES AND DOCUMENTATION.** Verizon will provide a Monthly Report and deliverables as described in an Engagement Letter.

3. **CONDITIONS.** Delivery of the Services by Verizon is predicated on the following conditions:
   - Customer is solely responsible for providing the operating systems (Windows, *nix, Mac, etc.) in the target environment, and to be responsible for deploying and installing the agent, and ensuring the accessibility of the agents via the Tanium platform.
   - Customer is responsible for purchasing enough licenses to cover Customer's full endpoint environment in order for the Endpoint Telemetry Analysis SLA to be valid.
   - Additional support beyond reasonable installation and maintenance of the deployed instances of Tanium on Customer's endpoints may require additional hours, which can be ordered through an Engagement Letter process at the hourly rate identified in the SOF.

Rapid Response Retainer Technical Service Description
Add-on Capability: Backbone NetFlow Collection

This service description describes Backbone NetFlow Collection, which may be selected as an Add-on capability pursuant to the Rapid Response Retainer base program (see Rapid Response Retainer Statement of Work), and included in a SOF.

1. **SERVICE DESCRIPTION.** Verizon's Backbone NetFlow Collection will capture 30 consecutive days of NetFlow data from the Verizon public IP network consisting of Customer IP address ranges listed in the Customer IP (CIP) schedule (the CIP Schedule) provided by Customer as requested by Verizon. Analysis is not included in this collection. Customer may request that Verizon analyze traffic patterns and telemetry related to Customer's identified IP addresses to identify possible indications of unwanted activity, pursuant to an Engagement Letter. Scope and pricing will be outlined in an Engagement Letter and will be provided pursuant to the hourly rates identified in the Rapid Response Retainer SOF (rate for RISK Services).

2. **DELIVERABLES AND DOCUMENTATION.** The Backbone NetFlow collection Add-on does not include any deliverables, however if analysis is requested by Customer, any reports will be described in an Engagement Letter.

3. **CONDITIONS**. Customer must provide a fully completed and executed CIP Schedule.

RAPID RESPONSE RETAINER SECURITY TECHNICAL ADVISORY OPTIONS

Following Onboarding, Customer may order any of the Services described below. The ordered Services will be provided with the number of Hours stated in an Engagement Letter.

- **Governance, Risk and Compliance – Security Technical Advisory options:**
  - Contact your Sales Representative for more information
- **Payment Card Industry – Security Technical Advisory Options:**
  - Payment Card Industry (PCI) Technical Advisory Services (see below)
- **Security Infrastructure – Security Technical Advisory options:**
  - Contact your Sales Representative for more information
- **Threat and Vulnerability Management – Security Technical Advisory options:**
  - Application Vulnerability Assessment (see below)
  - Internal Network Penetration Testing (see below)
  - Wireless Vulnerability Assessment (see below)
- **RISK Services – Security Technical Advisory options:**
  - Attack Detection Assessment (see below)
  - Incident Response Capability Assessment (see below)
  - Emergency Services (see below)
  - Espionage Health Check (see below)
  - Incident Analytics (see below)
  - Malcode Analysis (see below)
  - Retail Health Check (see below)

Rapid Response Retainer Technical Service Description
Payment Card Industry ("PCI") Technical Advisory Services

1. **Scope of Work.**
   1.1. Verizon will provide PCI data security standard ("PCI DSS") technical advisory services to Customer as described herein. Verizon will act in an advisory capacity providing Customer with on-going guidance pertaining to PCI DSS compliance, including maintenance of such compliance. Verizon will make remediation recommendations and draft written Deliverables as specifically requested by Customer. Verizon will provide Customer with technical advisory support if Customer chooses to implement remediation recommendations. Technical advisory support will consist of such activities as reviewing Customer's remediation plan and writing/updating policies and procedures associated with Customer's remediation activities.

   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, and meeting location (i.e. on site or remote). At or before the kickoff meeting, Customer shall provide a list of contact personnel with "after hours" emergency contact numbers and on-site authorization documentation (where applicable).

2. **Deliverables and Documentation to be produced by Verizon.** Verizon will provide, as requested by Customer, documentation that describes the Technical Services assistance and/or guidance provided by Verizon for the engagement.

3. **Documentation to be produced by Customer and Customer Obligations.** Delivery of the Technical Services by Verizon is dependent on Customer's appointing a single point of contact 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.

4. **Assumptions.** Delivery of the Technical Services by Verizon is predicated on the following assumptions and conditions:
   4.1. If the number of hours required to draft the Deliverables exceeds the hours specified in the Engagement Letter, Customer will execute a mutually agreeable amendment to the Engagement Letter such that Verizon can complete the Deliverables;
   4.2. The Technical Services are based on Verizon's understanding of Customer's requirements as documented in an Engagement Letter. Should the scope of the Project change, Verizon will continue work only after mutual execution of an amended Engagement Letter; and
   4.3. Customer is responsible for the implementation of any changes under the Engagement Letter to applications or devices managed by Customer or Customer's service providers.

THREAT AND VULNERABILITY MANAGEMENT - SECURITY TECHNICAL ADVISORY OPTIONS:

See below for descriptions of:

- Application Vulnerability Assessment
- Internal Network Penetration Testing
- Wireless Vulnerability Assessment

Rapid Response Retainer Technical 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 Technical 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.** 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 Technical 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 Technical 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 Technical 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 Technical Services.

4.3 Verizon will utilize its own laptops with disk or volume encryption employed for any Customer data stored during the Project.

Rapid Response Retainer Technical Service Description

Internal Network Penetration Testing

1. **Scope of Work.**

1.1. **Internal Network Penetration Testing.** The Project consists of network penetration testing (the "Technical 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 technical advisors 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).** 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 Technical 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 Technical 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 Technical 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 Technical 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 Technical Services will be performed remotely by Verizon, unless otherwise agreed.

Rapid Response Retainer Technical Service Description

Wireless Vulnerability Assessment

1. **Scope of Work.**

1.1 **Wireless Vulnerability Assessment.** The Project consists of wireless vulnerability assessment (the "Technical Services"). The Technical 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 Technical 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).** 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 Technical 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 Technical 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 Technical 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 Technical Services.

4.3 Verizon will utilize its own laptops with disk or volume encryption employed for any Customer data stored during the Project.

RISK SERVICES - SECURITY TECHNICAL ADVISORY OPTIONS:

See below for descriptions of:

- Attack Detection Assessment
- Incident Response Capability Assessment
- Emergency Services
- Espionage Health Check
- Incident Analytics
- Malcode Analysis
- Retail Health Check

Rapid Response Retainer Technical Service Description

Attack Detection Assessment

1. **Scope of Work.**

1.1. **Attack Detection Assessment.** The attack detection assessment services ("Attack Detection Assessment") is intended to assist Customer in measuring its capability to recognize and react to cyber-attacks. Verizon will evaluate Customer's operational incident-handling procedures. Attack Detection Assessment includes six phases that are cumulative in nature, providing multiple overlapping analyses of the strengths and weaknesses of Customer's operational incident handling capabilities.

1.1.1. **Phase 1: Defensive Countermeasures.** During phase 1, Verizon will review the selection, positioning and configuration of Customer's in-place security technologies including but not limited to firewalls, host and network-based intrusion detection, beacon identification and anti-virus. Verizon will provide a profile of Customer's defensive and threat hunting capabilities. Verizon will review Customer's event logging and alerting technologies such as security event management ("SEM") tools and intelligence integration platforms. Verizon will perform an on-site physical security inspection at one Customer location as defined in the Engagement Letter under the supervision of a designated Customer point of contact.

1.1.2. **Phase 2: Cyber Security Event Visibility.** Verizon will identify gaps in Customer's cyber security event detection which enable such events to go undetected. Phase 2 involves the correlation of Verizon cyber intelligence sources against Customer internet communications (e.g., firewall logs, netflow, etc.) for a sample period of up to 30 days (retroactive). In Phase 2, Verizon will benchmark the effectiveness of Customer's cyber security event capture methods. Phase 2 will require the completion and execution of a Customer IP schedule ("CIP").

1.1.3. **Phase 3: Incident Classification.** Verizon will perform a review of Customer's incident classification process documentation and will perform in-person interviews with identified Customer personnel. Verizon will evaluate the effectiveness of these process to detect cyber threats faced by Customer. Verizon will perform phase 3 at Customer's location as defined in the Engagement Letter.

1.1.4. **Phase 4: Intel Fusion.** Verizon will measure the effectiveness of cyber intelligence contained in Customer's operational incident handling processes. Verizon will evaluate Customer's ability to correlate cyber intelligence artifacts against cyber security event log streams. Verizon will review Customer's intelligence sources, data collection mechanism(s), archive and retention platforms, vetting and overall intelligence integration across log streams. Verizon will provide recommendations, if required, for changes to the collection, handling and application of cyber intelligence artifacts (i) to enable earlier detection of attacks in motion, (ii) during pre-attack research and (iii) to provide early indication of a possible intrusion or data theft. Phase 4 will be conducted on Customer's premises as defined in the Engagement Letter and will involve review of documentation and one-on-one interviews with identified Customer personnel.

1.1.5. **Phase 5: Visualization and Situational Awareness.** Verizon will test Customer's selection, deployment, configuration and usage of visualization tools. Verizon will perform

manual inspection of the visualization tools and platforms, walk through examples and interview identified Customer personnel. In phase 5, Verizon will evaluate Customer's application of these tools.

1.1.6. **Phase 6: Incident Triage.** Verizon will review the process utilized by Customer's operational incident handling personnel, or Computer emergency readiness team ("CERT"), in handling potential security incidents. Verizon will review how Customer's incident handling activities map to the existing Customer incident response plan. In phase 6, Verizon will evaluate Customer's staff's technical skillset, toolsets and familiarity with their role/function within documented policy. Verizon will review the quality and timeliness of cyber security incident information collection and documentation, as provided to CERT staff, to confirm the information is properly actionable. Verizon will evaluate the implementation and effectiveness of Customer's device tuning and optimization as a result of an incident. Verizon will conduct phase 6 at Customer's location as defined in the Engagement Letter and will involve a review of Customer's documentation as well as one-on-one interviews with identified Customer personnel.

During any phase, Verizon will communicate to Customer's point of contact significant weaknesses or points of security exposure as may be identified by Verizon.

1.2. **Project Management.** Verizon will work with Customer to schedule a kickoff conference call to initiate the Project. Verizon and Customer will collaborate to set the agenda and determine required stakeholders and other attendees. During or before the kickoff call, Customer will provide a list of appropriate contact personnel with "after hours" emergency contact numbers, and appropriate on-site authorization documentation (where applicable). The output of the kick off call will be an agreement on the resources, dates, times, and locations for the tasks described.

2. **Deliverables and Documentation to be produced by Verizon.** Upon completion of the Attack Detection Assessment, Verizon will furnish assessment findings and conclusions in the form of a "Management Report" including actionable recommendations to improve situational awareness related to cyber-attacks in motion and feedback on how Customer's current incident handling capabilities are appropriate to the size and business of the Customer.

3. **Documentation to be produced by Customer and Customer Obligations (if any).** Delivery of the Technical Services by Verizon is dependent on Customer's performance of the following:
   3.1. Customer will appoint a single point of contact 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 be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data; and
   3.3. Customer must complete and execute a CIP prior to the initiate of Attack Detection Assessment.

4. **Assumptions (if any).** Delivery of the Technical Services by Verizon is predicated on the following assumptions and conditions:
   4.1. Customer is responsible for the implementation of any changes under the applicable Engagement Letter to applications or devices managed by Customer or Customer's service providers; and
   4.2. Attack Detection Assessment will be performed during the hours defined in the Engagement Letter.

Rapid Response Retainer Technical Service Description

Incident Response Capabilities Assessment

1. **Scope of Work.**

1.1. **Incident Response Capabilities Assessment.** Verizon's incident response capabilities assessment ("IR Capabilities Assessment") will review and assess Customer's current policies, processes and procedures, work- flows, and capabilities (collectively the "Plans"), related to Customer's incident response ("IR") program. Verizon will focus the IR Capabilities Assessment on Plans surrounding information technology ("IT") security alerts and events that meet the threshold required to invoke Customer's IR processes. The IR Capabilities Assessment will be delivered in three (3) phases as described below:

1.1.1. **Phase I: Review Customer's IR Documentation.** During phase 1, Verizon will review Customer's documented policies, procedures, work flows, and any other documentation related to the Plans. Verizon will review the Plans against generally accepted industry practices for incident response. The information that will be included in the IR Capabilities Assessment will be grouped into the following six categories:

- Planning and preparation;
- Detection and classification;
- Collection and analysis;
- Containment and eradication;
- Remediation and recovery; and
- Assessment and reporting.

The purpose of the review will be to identify gaps in Customer's existing Plans, such as roles and responsibilities of IR stakeholders, escalation and communication processes, incident handling coordination measures, and other functions critical to executing an IR process.

1.1.2. **Phase 2: Interview Customer IR Stakeholders.** During phase 2, Verizon will work with Customer to identify all relevant IR stakeholders for the organization. Customer will schedule interviews at mutually agreeable times in which Verizon will collect additional information and institutional knowledge about any undocumented or informally-applied IR processes and procedures. Examples of relevant IR stakeholders may include, but are not limited to, personnel from external entities or business partners and the following Customer organizations:

- IR and/or security teams;
- IT management;
- Help desk / service desk;
- Legal;
- Human resources;
- Corporate communications / public relations;
- Governance, risk, and compliance;
- Corporate or physical security;
- Loss prevention;
- Business continuity and disaster recovery;
- Internal audit;
- Executive management; and
- Other stakeholders as applicable to the organization.

1.1.3. **Phase 3: Review Customer's IR Tools and Environment.** During phase 3, Verizon will work with Customer to identify all hardware and software tools, systems, and platforms (collectively "IR Tools") leveraged by Customer for IR purposes, within four main categories:

- Incident detection and validation;
- Evidence collection and analysis;
- Incident reporting; and
- Key performance indicators reporting for incident management.

Verizon will assess all relevant IR Tools to determine their suitability for IR, investigative and incident management purposes.

1.2. **Project Management.** Verizon will work with Customer to schedule a kickoff conference call to initiate the Project. Verizon and Customer will collaborate to set the agenda and determine required stakeholders and other attendees. During or before the kickoff call, Customer will provide a list of appropriate contact personnel with "after hours" emergency contact numbers, and appropriate on-site authorization documentation (where applicable). The output of the kick off call will be an agreement on the resources, dates, times, and locations for the tasks described.

2. **Deliverables and Documentation to be produced by Verizon**. Upon completion of the engagement, Verizon will produce a "Management Report" which will include observations from each of the three phases and provide recommendations designed to enhance, mature, or improve Customer's IR capabilities. The Management Report may, at Customer's request, including a recommendation for training course(s) for Customer's security personnel.

3. **Documentation to be produced by Customer and Customer Obligations (if any).** Delivery of the Technical Services by Verizon is dependent on Customer's performance of the following:
   3.1. Customer will appoint a single point of contact 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 be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data;
   3.3. Customer will provide appropriate on-site authorization approval and documentation;
   3.4. Customer will provide identification of and access to IR-relevant technologies, systems, and locations of related IR data; and
   3.5. Customer will schedule interviews as described in phase 2 above.

4. **Assumptions.** Delivery of the Technical Services by Verizon is predicated on the following assumptions and conditions:
   4.1. Customer is responsible for the implementation of any changes to documented policies, processes and procedures and IT Tools managed by Customer or Customer's service providers as recommended in the Management Report; and
   4.2. Technical Services will be performed at the Customer sites and during the hours as defined in the Engagement Letter.

Rapid Response Retainer Technical Service Description
Emergency Services

1 Scope of Work.

1.1 **Emergency Services.** (Uses Hours as required)

1.1.1 An Engagement Letter is required for Emergency Services.

1.1.2 **On Site Response with In-Transit SLA.** When the Parties agree that a member of Verizon's investigative team must travel to a Customer Site, the Verizon investigative team member will be "in- transit" to the Customer Site within twenty-four (24) hours of (a) Customer's execution of the Engagement Letter and (b) Verizon's procurement of all required travel documentation and Customer's approval if required. "In-transit" means the investigative team member is traveling to the Customer Site. The in- transit SLA clock begins when (a) and (b) are both complete and stops when the investigative team member is in-transit. Verizon's investigative team phone support is available while the investigative team member is in-transit.

1.2 **Emergency Services Phases.** Customer and Verizon will determine which of the following phases are required for an Emergency Services Project:

1.2.1 Incident Response Phase. The goal of the incident response phase is to contain and investigate an incident as necessary to bring the affected systems back into a trusted state. A key element in the incident response phase involves data collection by Customer or Verizon in the immediate aftermath of an incident. This phase can take place either onsite or remote, depending on the nature of the incident. Verizon will work with the Customer and will determine the appropriate response given the specific incident information provided by Customer, including:

1.2.1.1 Notification: Verizon will identify and alert the appropriate Verizon and Customer personnel of the incident so that a proper response can be formulated;

1.2.1.2 Assessment: Verizon will define the scope of the incident and identify data sources relevant to the incident. Data may be collected to help assess the severity of the incident and the necessary or recommended response. Collection and analysis of this data provides information to help Customer make a business decision on how to proceed with the incident response process.

1.2.1.3 Response and Acquisition: Verizon will respond based on the decisions made by Customer and Verizon during the assessment. A response may include acquiring data from the affected system(s) for in-depth forensic analysis or increasing network monitoring to gather additional data. During response and acquisition, depending the nature and severity of the incident, Verizon may collect and preserve data of evidentiary value, establish a chain of custody for the data, and securely transport such data to a Verizon's forensic lab for further analysis.

1.2.1.4 Verizon Responsibilities. Verizon's response may include the following elements, depending on the nature of the incident:

1.2.1.4.1 Analysis: Verizon's analysis of relevant data to determine the source of the incident, its cause (program error, human error, or deliberate action), and its effects;

1.2.1.4.2 Containment: Verizon will work with Customer to prevent further data loss, and the effects of the incident from spreading to other computer systems and computer networks in the Customer's environment; and

1.2.1.4.3 Eradication: Verizon will work with Customer to remove instances of identified malware, or unprotected sensitive data so that the affected systems can be properly secured and brought back online by the Customer.

1.2.1.4.4 Report: Depending upon the nature of the engagement and Customer's request or if otherwise required, upon completion of the incident response phase, Verizon will produce a statement of preliminary findings (the "Preliminary Finding Report").

1.2.2 Forensic Analysis Phase. During the forensic analysis phase, Verizon will perform a further in-depth analysis on the data that was acquired during the incident response phase as well as gathering additional data for analysis. The objective of the forensic analysis is to reveal the source of the incident, method of intrusion, the extent to which sensitive data has been compromised, and any other details relevant to the investigation. This phase can take place either onsite or remote. Verizon will use analysis tools, knowledge of operating systems and file systems, and knowledge of vulnerabilities to identify evidence that can be used to determine the origin and details of the incident in accordance of the scope and objectives as stated in the Engagement Letter.

1.2.2.1 Methodology. Verizon will perform an analysis of the data to extract evidence. This analysis will be performed using a combination of open source, commercially available, and Verizon proprietary tools. During the analysis, Verizon will use several techniques to identify data including but not limited to:

- Analysis of allocated and unallocated files and directories;
- Timeline of file, application, and network activity;
- Analysis of unallocated file system space;
- Analysis of binaries to identify malicious code, determine its source and capabilities; and
- Analysis of file system structures to find evidence of anti-forensics activities.

1.2.2.2 Forensic Report. At the conclusion of the forensic analysis phase, Verizon will provide Customer with a management report ("Forensic Report") containing the specific findings of the investigation.

2. **Deliverables and Documentation to be produced by Verizon.** Verizon will provide:

2.1 Preliminary Finding Report

2.2 Forensic Report

Rapid Response Retainer Technical Service Description

Espionage Health Check

1. **Scope of Work.**

1.1 **Espionage Health Check.** With "Espionage Health Check" Verizon conducts an investigation on Customer's in scope systems, IP ranges, or applications to identify evidence of a security breach in progress. Espionage Health Check takes a three phased approach to determine if Customer is experiencing a security breach in progress, unauthorized access and/or communication with known bad actors consistent with recent Verizon investigations. The Technical Services will include an onsite inspection, a physical inspection, and a logical inspection of Customer's in scope systems and hardware.

1.1.1 **Phase 1: Cyber Intelligence Correlation 'Go-Forward'.** Phase 1 involves the collection and cross- correlation of Verizon's intelligence set against Customer device logs, netflow for the IP addresses shown in Customer's CIP Schedule, and Internet communications during the term of the Project. For a specified period (to be agreed to between Customer and Verizon prior to phase 1 commencing) while investigative work is underway, Verizon will collect log information from Customer systems and from our public IP backbone from the IP addresses shown in the CIP Schedule. These sources will be matched from time to time as often as Verizon deems necessary within the period for this phase to identify potentially malicious activity in-progress. Findings that Verizon deems to be critical will be shared with the Customer as soon as practicable following discovery.

1.1.2 Phase 2: Cyber Intelligence Correlation 'Retroactive'. Phase 2 will examine logs of historical data from Customer's systems provided from Customer and historical data from Verizon's public IP backbone from the IP addresses shown in the CIP Schedule. Such historical data will be limited to a specified number of months from within the most recent twelve months as agreed to between Customer and Verizon prior to phase 2 commencing (collectively, the "Phase 2 Data"). Verizon will collect and process Phase 2 Data, in order to focus on previous or earlier connections with known bad actors. Verizon will analyze the Phase 2 Data to: a) look into Customer's network communications patterns over time, and b) correlate potentially suspicious connections to Customer's physical systems and hosts. This Phase 2 review will be conducted on a one-time-only basis.

1.1.3 Phase 3: Boots-on-the-Ground Verification. In phase 3, Verizon will take a sampling of Customer's data through forensics images or logical file copies of Customer systems, and conduct in-depth digital forensic analysis of the data. Verizon will collect digital images of a limited number of Customer-identified critical systems, as determined by Verizon and Customer, that are typically involved in cyber espionage attacks. These may include but are not limited to Customer domain controllers, sensitive data stores, remote access and transaction processing systems. This is a partially invasive action and should be scheduled after usual business hours or during a suitable maintenance window, as designated by Customer. The Customer- provided list of Customer systems to be included in the sample will be refined as phases 1 and 2 are completed.

Verizon cannot determine the exact level of effort required for this Project without knowing the amount of data, systems, or the results of the analysis from phase 1 or phase 2. Verizon will stay in communication with the Customer throughout the Project and, if additional Hours are required, Verizon will discuss with the Customer and add such Hours pursuant to an Engagement Letter. If Customer requires further assessment and investigative work, such services may be provided pursuant to another Technical Services engagement.

1.2 **Project Management.** Verizon will appoint a Project Manager who 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 remote. Verizon will produce an agreed project plan, which specifies required resources (Verizon and Customer), dates, times, and locations for the tasks described (the "Project Plan").

2. **Deliverables and Documentation to be Produced by Verizon.** Verizon will provide:

2.1 The Project Plan; and

2.2 A "Management Report" that summarizes the results of the analysis, identifies any "bad actors" and questionable activity detected and makes recommendations of reinforcements, countermeasures and monitoring Customer may employ to help defend its organization from cyber-espionage.

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

3.1 Designate a single point of contact to facilitate execution of the Customer's obligations to ensure the Project is delivered within the agreed time-frame;
3.2 Provide access to appropriately qualified and knowledgeable Customer personnel and third party business partners if necessary, for interview and documentation as required;
3.3 Permit access to its in-scope systems and applications as required;
3.4 Provide Verizon with copies of all configuration information, log files, intrusion detection events, and other data relevant to the in-scope Technical Services;
3.5 Provide Verizon a list of all systems relevant to the in-scope Technical Services;
3.6 Provide a secure office or work area equipped with desks, chairs, telephones, and laptop computer connections (or analog telephone lines, as Verizon specifies) for use by Verizon while working on-site at Customer premises;
3.7 Be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, back-up and security of stored data; and
3.8 Complete and execute a CIP Schedule prior to the initiation of Espionage Health Check.

Rapid Response Retainer Technical Service Description

Incident Analytics

1. Scope of Work.

1.1 **Incident Analytics Service.** Verizon will assist Customer with Customer's collection, classification and analysis of Customer's security incidents ("Incident Data") in accordance with the vocabulary for event recording and incident sharing ("VERIS") framework. VERIS is an industry standard framework designed to provide a common language for describing security incidents in a structured and repeatable manner. More information can be found at http://veriscommunity.net/index.html.

Verizon will provide support to Customer as follows:

1.1.1 Verizon VERIS Framework Implementation Support and Training

1.1.1.1. Verizon will assist with the development of Customer's plan to implement the VERIS framework so that Customer can gather and analyze Incident Data collected from Customer's security incidents. Verizon will subsequently assist Customer with incorporating VERIS into Customer's existing investigative response ("IR") tools and processes. To achieve this, Verizon will meet with Customer stakeholders to:

1.1.1.1.1 obtain an overview of Customer's current IR tracking process;

1.1.1.1.2 understand Customer Incident Data points that are currently being tracked;

1.1.1.1.3 gather information on how the VERIS framework might be incorporated;

1.1.1.1.4 identify potential roadblocks that may be encountered and identify where Customer Incident Data will be collected from;

1.1.1.1.5 determine the number of Customer business groups or departments that will need to be included in the classifications; and

1.1.1.1.6 determine how many Customer Incident Data sources or processes there are within Customer's organization.

1.1.1.2 Following collection of the information, Verizon will then provide training to Customer to aid understanding of how to implement the VERIS framework into Customer's organization. The training will provide an overview of the VERIS framework, both conceptually and in practice. Verizon will deliver this training to Customer's employees only.

1.1.1.3 The total maximum hours for the services described in this section "Verizon VERIS Framework Implementation Support and Training" will be no more than the number of hours specified in the Engagement Letter.

1.1.2 Incident Classification (if specified in the Engagement Letter)

1.1.2.1 Verizon will support Customer with incident classification by providing Customer with detailed information regarding the VERIS framework, recording Customer's in-scope Incident Data in the "VERIS language," and

assisting Customer with performing the classifications correctly and uniformly in accordance with the VERIS framework across Incident Data as further detailed in the sub sections below. In order to provide this service, Customer shall present Verizon with access to the in-scope Incident Data that Customer requires to classify according to the VERIS framework. Verizon will assist Customer on the transfer and preparation of the Incident Data.

1.1.2.1.1 Understanding the VERIS framework. Verizon will provide training to Customer on utilization of the VERIS framework. The training will be on the four sections of the VERIS framework, each of which captures a different aspect of a security incident. The sections are: a) ”demographics,” such as the date of the incident, how serious it was, the region in which it occurred and Customer’s vertical industry; b) ”incident classifications” using metrics to detail the series of events that an incident comprises, who was affected and what was done, using the VERIS A4 model (Actors, Action, Asset, and Attribute); c) ”discovery and mitigation” analyzes the events immediately following an incident and the lessons learned. Metrics include a timeline, how the incident was discovered, the resources used, the controls used and whether they were adequate; and d) “impact analysis” which categorizes the varieties of losses experienced; estimate their magnitude; and captures a qualitative assessment of the overall effect on the organization.

1.1.2.1.2 Recording the In-Scope Incident Data and Validation. At Customer’s option and where specified in the Engagement Letter:

1.1.2.1.2.1 If Customer has performed Incident Classification, Verizon will assist Customer to record the Incident Data in the VERIS language. Verizon will also assist Customer in its classification of backlogged Incident Data that Customer provides to Verizon. Verizon will review Customer’s classifications of incidents up to the number specified in the Engagement Letter and provide feedback to Customer on classification. Once Customer has demonstrated that Customer understands how to classify the test incidents, Verizon will give Customer time to complete Customer’s in-scope Incident Data. Once the classifications have been completed on the in-scope Incident Data, Verizon will assist Customer to review random validations of the incidents that were classified to understand if the classifications were done pursuant to the VERIS framework; or

1.1.2.1.2.2 If Verizon has performed Incident Classification, Verizon will take Customer’s in-scope Incident Data and record it in the VERIS language. Verizon will assist Customer in classification of backlogged Incident Data that Customer provides to Verizon. Once Verizon has completed classification of the in-scope Incident Data, Verizon will demonstrate to

Customer that the classifications were done pursuant to the VERIS framework by performing several random validations of the incidents that were classified.

1.1.2.2 The total maximum hours for the services described in this section ”Incident Classification” will be no more than the number of hours specified in the Engagement Letter.

1.1.3 Data Analysis (if specified in the Engagement Letter).

1.1.3.1 Verizon will assist Customer with analyzing Incident Data. For the initial analysis, Customer shall provide Verizon with the in-scope incidents classified pursuant to the VERIS framework. (Note: Verizon may have performed the classifications). Once the statistical analysis of the Incident Data has been concluded, the resulting findings will be summarized. At this point, Verizon will perform an in-depth analysis of the classified dataset to identify trends, commonalities, and security weaknesses, common failures or root causes. By identifying the trends and patterns in the dataset, Verizon will assist Customer in identifying justified treatment options that may reduce similar incidents from occurring in the future. Verizon will summarize the result of its analysis in a report of findings (the “Data Analysis Report”).

1.1.3.2 The total maximum hours for the services described in this section ”Data Analysis” will be no more than the number of hours specified in the Engagement Letter.

1.1.4 Comparative Data (if specified in the Engagement Letter)

1.1.4.1 Utilizing the in-scope incidents classified pursuant to the VERIS framework, and any data analysis that may have been done, Verizon will provide Customer with data comparisons against those in the Verizon master database (the “Comparative Data Report”). The Verizon database has detailed security incidents which are collected in collaboration with global organizations and ongoing Incident Data collected within the VERIS framework globally. The Comparative Data Report will show where Customer stands in relation to other companies of a similar stature (i.e. same industry, and/or size, and/or location, etc.) and will allow Customer the ability to make decisions about the status and direction of Customer’s security program. (Note: Verizon may have performed the classifications).

1.1.4.2 The total maximum hours for the Comparative Data services described in this section ”Comparative Data” will be no more than the number of hours specified in the Engagement Letter.

1.2 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, and meeting location (i.e. on site or remote). At or before the kickoff meeting, Customer shall provide a list of contact personnel with “after hours” emergency contact numbers and 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 Project tasks (the “Project Plan”).

13 The Technical Services will be provided remotely unless otherwise agreed in the Engagement Letter.

2. **DELIVERABLES AND DOCUMENTATION TO BE PRODUCED BY VERIZON** Verizon will provide:

   2.1 the Project Plan;

   2.2 the Data Analysis Report if applicable; and

   2.3. the Comparative Data Report if applicable.

3. **DOCUMENTATION TO BE PRODUCED BY CUSTOMER AND CUSTOMER OBLIGATIONS.** Delivery of the Technical Services by Verizon is dependent on Customer's performance of the following:

   3.1 Customer will provide to Verizon addresses of networked devices to be tested within the scope of the Technical Services at least seventy-two (72) hours or more prior to the scheduled commencement of the Technical Services;

   3.2 Customer will provide Verizon with copies of all configuration information, log files, intrusion detection events, and other data relevant to the in-scope Technical Services;

   3.3 Customer will provide access to the in-scope Incident Data (classified in the VERIS format, if required) that Customer is wishing to classify, analyze, or conduct a comparative analysis on;

   3.4 Customer will be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and back-up and security of stored data; and

   3.5 Customer will be responsible for ensuring that the Incident Data does not contain any personally identifiable information.

4. **ASSUMPTIONS** Delivery of the Technical Services by Verizon is predicated on the following assumptions and conditions:

   4.1 Access to the Customer contacts and resources are 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 Technical Services.

   4.2 The Incident Data does not contain any personally identifiable information.

Rapid Response Retainer Technical Service Description
Malcode Analysis

1 Scope of Work.

1.1 **Malcode Analysis.** (Uses Hours as Required)

1.1.1 An Engagement Letter is required for malcode analysis.

1.1.2 Malcode analysis provides analysis of files that Customer suspects might be malicious. Malcode analysis is limited as described herein and does not replace an Emergency Services forensic analysis. All files uploaded for malcode analysis must be isolated as individual files and may not be uploaded as part of a memory dump or network capture. Verizon will analyze no more than one file per 24-hour period.

1.1.3 Customer will upload malicious or suspicious files to the Verizon server for analysis. Instructions on how to upload files to the Verizon server will be provided to the Customer during the Onboarding session.

1.1.4 **Analysis.** Malcode analysis will typically focus on the interactions of the malcode with Customer's system. Verizon will attempt to determine the functionalities of suspected malicious files. Depending on the nature of the suspected malware functionality, the analysis may include identification of communication channels, a listing of indicators of compromise, and malware response guidelines. Malcode analysis may include the following, as determined by Verizon:

1.1.4.1 Code anatomy, which provides an overview of the malware binary content;

1.1.4.2 Behavioral analysis, which is a high level overview of the malcode's functioning with the objective of assisting in identifying system changes caused by the malcode and/or communication channels (e.g., IP addresses and domain names) utilized by the malcode; and

1.1.4.3 Malware intelligence analysis, which leverages Verizon's intelligence datasets to determine if the malware is already known and/or affiliated with known incidents or actors.

1.1.5 **Report.** Verizon will issue a report at the end of the analysis of the submitted code sample ("Malcode Analysis Report"), which will contain any identified findings, indicators of compromise and recommendations for additional analysis.

1.1.6 **Malcode Analysis SLA.** Within 24 hours of receipt of a signed Engagement Letter and Customer's suspect files at the Verizon server, Verizon will perform an analysis of the files and provide Customer with the Malcode Analysis Report. If additional analysis is required after the first 24 hours, Verizon will continue with the service as described in the Engagement Letter.

2. **Deliverables and Documentation to be produced by Verizon.** Verizon will provide:

2.1 Malcode Analysis Report

Rapid Response Retainer Technical Service Description

Retail Health Check

1. **Scope of Work.**

1.1 **Retail Health Check.** The Project consists of a retail health check (the "Technical Services"). Verizon will conduct an investigation at the Customer store locations identified in the Engagement Letter (the "Locations"), to test for evidence of a security breach. The Technical Services will consist of two phases of examination and a third phase providing knowledge transfer to Customer.

1.1.1 **Phase 1: Onsite Review and Assessment.** During phase 1, Verizon will visit Customer's Locations to discover evidence of a security breach affecting Customer's payment card processing and/or Sensitive Data. "Sensitive Data" consists of:

- Credit card numbers
- Credit card track data
- Other Customer data, subject to mutual agreement.

1.1.1.1 Major activities in this phase will consist of systems and network inspection, evidence collection, disk and memory analysis, and review of select other types of material evidence, which may include:

1.1.1.1.1 Forensic imaging of point of sale ("POS") devices, from a sampling of store locations as determined by Verizon;

1.1.1.1.2 Analysis of a sampling of system memory modules to identify unauthorized processes that may be running and evidence of potential malware;

1.1.1.1.3 Examination and correlation of active network connections and data transfer flows involving POS systems for evidence of potentially malicious activities;

1.1.1.1.4 Examination of system process information to identify potentially malicious tampering with authorized transaction related processes;

1.1.1.1.5 Review to identify suspicious log activity with POS;

1.1.1.1.6 Review of system scheduled processes to identify potential malware persistency and unusual activity;

1.1.1.1.7 Performance of registry analysis of Customer's Windows systems to identify possibly embedded malware and unauthorized software; and

1.1.1.1.8 Analysis of the master file table for created known files exhibiting unusual or out of place characteristics.

1.1.1.2 To minimize impact to Customer's store operations, material evidence will be collected and preserved from Customer systems and securely transmitted to Verizon's forensics lab to conduct an analysis of collected information.

1.1.2 **Phase 2: Internet Traffic Pattern Analysis.** Verizon will analyze Customer's netflow data (as identified in the CIP Schedule and further described in the Engagement Letter) for correlation against Verizon's "indicators of compromise" ("IOC") database. The IOC database is a compilation of data collected by Verizon from internal and external sources.

1.1.2.1 Verizon will examine the netflow metadata (source and destination IP addresses, source and destination ports), packet count and bytes (in Customer's communications, both inbound and outbound), to detect known threat actors, as well as traffic patterns that are considered malicious.

1.1.2.2 Verizon will also analyze Customer's log data, as further described in the

Engagement Letter, to be provided by Customer in advance.

1.1.2.3 The Customer's log data (the "Logs") shall include Customer's logs exported from Customer's security information and event management ("SIEM") tool(s) for correlation against Verizon's IOC database for evidence of malicious activity.

1.1.2.4 Customer will load the Logs to an encrypted drive (to be provided by Verizon) and securely ship the drive to Verizon's forensic lab facility for in-depth analysis. Verizon will work with Customer to maintain proper evidence handling procedures and will establish and maintain appropriate chain of custody documentation for the Logs throughout the lifecycle of the Project.

1.1.2.5 Log data will consist of Customer data from an internet-facing device and include connection data such as source and destination IP addresses, and other data as reasonably required by Verizon.

1.1.3 **Phase 3: Knowledge Transfer.** Following the completion of phases 1 and 2, Verizon will combine the results of the analysis conducted during each phase and provide Customer with a summary of findings and recommendations related to the findings that may assist Customer with reinforcing security countermeasures where appropriate (collectively, the "Report"). Additionally, Verizon may provide Customer recommendations as to how Customer may monitor Customer's remaining infrastructure to identify unwanted activity.

1.2 **Project Management.** Verizon will work with Customer to schedule a kickoff conference call to initiate the Project. Verizon and Customer will collaborate to determine required stakeholders and other attendees and the agenda. 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 kick off call is an agreement on the resources, dates, times, and locations for the tasks described.

1.2.1 Customer will appoint a single point of contact or program management team to coordinate the Project activities with Verizon and ensure timely data flow and exchange of information required for execution of the Project within the agreed time frame.

2. **Deliverables and Documentation to be produced by Verizon (if any).** Verizon will provide the Report.

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

3.1 Customer will provide Verizon with copies of all configuration information, log files, intrusion detection events, and other data relevant to the Technical Services.

3.2 Customer will be responsible for the actual content of any data file, selection, and implementation of controls on its access and use, and security of stored data.

3.3 In advance of any on-site work, Customer will also provide Verizon with an understanding of the following regarding the in-scope locations:

- Store POS infrastructure;
- Payment card authorization request flow;
- Store-level architectures and variance by region; and
- Store and headquarters security architecture related to Customer's PCI environment.

4. **Assumptions (if any).** Delivery of the Technical Services by Verizon is predicated on the

following assumptions and conditions:

4.1 Customer is responsible for the implementation of any changes under this SOW to applications or devices managed by Customer or Customer's service providers.

4.2 Access to the Customer contacts and resources 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 Technical Services.

SAMPLE ENGAGEMENT LETTER AND IP ADDRESS DOCUMENT

ENGAGEMENT LETTER TEMPLATE

Rapid Response Retainer Engagement ID:

Engagement Letter is being issued pursuant to Rapid Response Retainer Statement of Work ("SOW") No. ____, and the related Agreement with the Contract ID#_____.

RE: Engagement Letter

Service Location:	*<TBD – SAMPLE ONLY>*
Scope of Work:	*<TBD – SAMPLE ONLY>*
Deliverable:	*<TBD – SAMPLE ONLY>*
Engagement Start Date:	*<TBD – SAMPLE ONLY>*
Hourly Rate/Hours:	*<TBD – SAMPLE ONLY>*

Verizon Point of Contact	Customer Point of Contact
<TBD – SAMPLE ONLY>	*<TBD – SAMPLE ONLY>*

CUSTOMER NAME

Authorized Signature: _____

Name (print): *<TBD – SAMPLE ONLY>*

Title: _____

Date: _____

THIS DOCUMENT MUST BE SIGNED BY AN AUTHORIZED CUSTOMER REPRESENTATIVE PRIOR TO ANY WORK COMMENCING FOR THE TECHNICAL SERVICES OUTLINED HEREIN.

Customer IP Address Schedule ("CIP Schedule") to the Rapid Response Retainer Statement of Work

1. **Description.** The Technical Services as described in the Rapid Response Retainer Statement of Work requires that Verizon perform Technical Services for Customer utilizing a list of Customer provided IP addresses (collectively, "CIP") as provided by the Customer below.

Location/Site	IP Addresses
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address
Enter Location / Site	Enter IP Address

2. **Customer Representations and Warranties related to the Technical Services and Customer IP Addresses provided.** Customer represents and warrants that:
   2.1 the Deliverables, documentation, and other information provided by Verizon in connection with the Technical Services requiring a CIP Schedule will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use of Verizon's public Internet service;
   2.2 the list of Internet IP addresses provided by the Customer contains only IP addresses that have been assigned or allocated for the exclusive use of Customer and/or affiliates of Customer over which Customer has control; and
   2.3 it has obtained or will obtain all legally required consents and permissions from users of CIP for Verizon's performance of the Technical Services requiring a CIP Schedule, including without limitation the collection, use, processing, analyses and disclosure to Customer of Customer's Internet traffic data.

In Witness Whereof, Customer has caused this CIP Schedule to be executed by its duly authorized officers or representatives, effective as of the date set forth below:

Click here to enter Customer's legal entity name **(Customer Signatory)**
Registered Office Address: Click here to enter Customer's legal address

Customer Signature:
Name: Name
Title: Title
Date: Click here to enter a date