Verizon Threat Intelligence Platform Service (VTIPS) Professional Service Description Incident Response and Forensics.

1 **Scope of Work.**

1.1 **Services Phases.** Customer and Verizon will determine which of the following phases are required for supporting a Customer during a suspected security concern:

1.1.1 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:

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

1.1.1.2 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.

1.1.1.3 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.

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

1.1.1.4.1 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;

1.1.1.4.2 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

1.1.1.4.3 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.

1.1.1.4.4 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").

1.1.2 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.

1.1.2.1 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.

1.1.2.2 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.** Any Deliverables are intended for Customer and Verizon use only. Customer may disclose a Deliverable to a third party pursuant to the Agreement's confidentiality terms. Verizon will provide:

2.1 Preliminary Finding Report

2.2 Forensic Report