Verizon Threat Intelligence Platform Service (VTIPS) Professional 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 Professional 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 Professional 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. Deliverables are intended for Customer and Verizon use only.** Customer may disclose a Deliverable to a third party pursuant to Verizon's confidentiality terms. 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 Professional 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 Professional Services;
3.5 Provide Verizon a list of all systems relevant to the in-scope Professional 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.