Verizon Threat Intelligence Platform Service (VTIPS) Professional 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**. 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. 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 Professional 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 Professional 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. Professional Services will be performed at the Customer sites and during the hours as defined in the Engagement Letter.