eSENTIRE

Service Description: OnDemand 24/7 Incident Response Service with 4-Hour Threat Suppression

1. Features and Capabilities

Purchase of the OnDemand 24/7 Incident Response Service ("**IR Service**") entitles Client to one or more years of program support (each 12-month period is a Contract Year) which will begin on the Service Commencement Date (defined on the Order Form). Each Contract Year of the IR Service will include: a) on-boarding call; b) engagement process for services; c) one IR Planning Service; c) committed response times for urgent services; d) eSentire digital forensics agents (referred to as the eSentire Agent(s) or the "**Agent**") deployment (in the first year and maintained in subsequent years); e) discounted hourly rate; and f) cyber intelligence. Each IR Service feature is detailed below:

1.1 Onboarding Call. Following the Parties' execution of an Order form, eSentire will schedule an onboarding call with Client to collect and discuss necessary information for service setup ("**On-boarding Call**"). This information may include: (a) Client contact information, including off-hours contact information and technical point of contact ("**POC**"); (b) service ordering and process for engagements; (c) a review of service level commitments and options; (d) select IR Planning Service; and (e) coordinate deployment of eSentire Agents. Following the On-boarding Call, Client may begin utilizing all IR Service components though four-hour threat suppression will not be available until Agent software has been deployed in Client's organization.

1.2 Engagement Process for Services. Client may contact eSentire for incident response, forensics analysis, malcode analysis, mergers and acquisitions assessments, human resource policy/corporate security/PII/or data exfiltration investigations, eDiscovery collection, post breach support, breach consulting, or other related security support services, by using the toll-free number ("**Hotline**") provided by eSentire during the ON-boarding Call. eSentire will return Client's call within two hours after its call to the Hotline. If Client is an active eSentire Managed Detection and Response ("**MDR**") customer, the eSentire Security Operations Center ("**SOC**"), may initiate Services on behalf of the Client when needed, obviating the need for Client to utilize the Hotline. During the return call, or following SOC engagement, eSentire will document the requested Service in an Engagement Letter (a sample form will be provided upon request), which will set forth a high-level scope of work, deliverables, hourly rate, and an estimated number of hours. If Client has specific data collection and storage requirements, Client must bring these to the attention of eSentire prior to execution of the Engagement Letter. Client also must specify whether it requires any data retention. If Client fails to do so prior to execution of the Engagement Letter, eSentire will follow its standard policy, which is to delete all Client's data in its possession utilizing applicable DoD standards, including, but not limited to forensic images, at the completion of the IR Services. Client must execute an Engagement Letter before any IR Services can commence. eSentire will invoice Client for IR Services on an hourly basis monthly in arrears at the hourly rate for the level of service selected on the Order Form. Travel and associated expenses are not included in the hourly rate and will be invoiced separately at cost, as incurred. All work will be performed remotely unless otherwise specified.

1.3 IR Planning Service. Each IR Service includes one IR Planning Service per Contract Year, and Client may choose from one of the three options below:

1.3.1 Incident Response Plan Development.

If selected, eSentire will provide Client an incident response plan ("IR Plan") template, following the Onboarding Call, via email. The IR Plan template will contain instructions and notes to guide the Client through completion. Client will have 180 Days following receipt of the IR Plan template from eSentire, to review and complete all applicable sections. During the development, Client should save any questions they may have, until completion of the template. It is the Client's responsibility to work with its legal advisors to take into consideration all applicable legal, privacy, and compliance/regulatory requirements. Sections of the IR Plan template for Client completion include (but are not limited to):

- Update Client's Full Name throughout the document,
- Version Control Section,
- Executive Sponsorship,
- Executive Leadership Titles/Roles,
- Emergency Response Threshold Guidelines,
- Contact List and War room details, and
- Link to System/Asset List.

Following completion of the draft IR Plan template, Client should send the draft IR Plan back to eSentire via email and request a review session to be scheduled. The session will be scheduled to take place over a one-hour call and is intended to work through any questions Client generated during plan completion. This call is not intended to perform an assessment of the draft IR plan or provide any content for areas that are gaps in Client's processes or procedures. Following the review call, if Client would like to schedule additional consulting time for analysis or further consulting regarding their draft IR Plan template, this can be ordered at the hourly rate, pursuant to an Engagement Letter.

1.3.2 Incident Response Plan Assessment.

If selected, eSentire will request Client send existing IR Plan to an eSentire email (to be provided). The IR Plan must be sent to eSentire by Client no later than 180 Days following the Service Commencement Date. eSentire will confirm receipt of the IR Plan and assign a resource to conduct an assessment. eSentire will then review and assess Client's documented policies, procedures, workflows, and any other documentation included in Client's IR Plan.

Within 30 Days of eSentire's receipt of Client's IR Plan, eSentire will email Client a redline to its IR Plan, which will include comments with any observations or recommendations that may assist in enhancing, maturing, or improving Client's incident response capabilities. eSentire will also offer a one-hour review call to go over the redlines sent by email. Client may use the review call to ask any questions they may have regarding the comments or recommendations. If following the review call, Client would like to schedule additional consulting time for analysis or further consulting regarding their IR Plan, this can be ordered at the hourly rate, pursuant to an Engagement Letter.

1.3.3 Tabletop Assessment.

Client also has the option of requesting a table-top exercise as their IR Planning Service option. Client should notify eSentire during the Onboarding call, that this is the option they wish to select, and the onboarding manager will schedule a time to conduct a planning call. The planning call will need to be conducted within the first 180 Days from the Service Commencement Date (unless otherwise mutually agreed). The purpose of the tabletop exercise is to provide the ability for Client to test its existing processes and procedures for responding to cyber-security

emergencies. During the planning call, eSentire will work with one or two Client contacts to customize an appropriate and realistic mock incident scenario. Following the planning call, eSentire will schedule a tabletop exercise to work through the incident scenario no later than 60 Days following the planning call. Following the tabletop exercise, eSentire will provide the Client a report summarizing the tabletop, findings, and any recommendations, via email.

IR Planning Services are not considered urgent services, are delivered during standard business hours, and are not subject to a service level agreement. Client's right to one annual IR Planning Service does not carry over from one Contract Year to any subsequent Contract Year. Client acknowledges that, if Client fails to exercise such right during the time periods identified above, Client will forfeit such right with respect to that Contract Year.

1.4 Committed Response Times for Urgent Services. After the On-boarding call is completed, Client may request urgent incident response Services from eSentire. Using eSentire Agent's remote forensic analysis technology, most issues can be handled remotely through eSentire threat suppression activities. For urgent service requests requiring Threat Suppression, eSentire will begin activities within four hours after its receipt from Client of an executed Engagement Letter and confirmation of installation of the Agents, if not already complete. Threat Suppression includes initial analysis, beginning to identify and preserve evidence, and initiating containment measures. Threat suppression does not mean residual malware may be fully cleaned from all systems. Complete eradication and environment remediation are outside the scope of Threat Suppression. If required, any additional remediation and forensics work following initial Threat Suppression activities will be set forth in a separate Engagement Letter for execution by Client.

If Client requires on-site support for urgent service requests that cannot be addressed using Threat Suppression, eSentire will arrange for its personnel to be enroute to Client's designated location within the United States or Canada within 24 hours after eSentire's receipt from Client of an executed Engagement Letter (and if required, all associated travel approvals from Client).

1.5 Agent Deployment. The IR Service includes deployment of Agents to be installed on Client assets. The standard Service includes 100 Agents, unless otherwise stated on the Order Form. eSentire will coordinate with Client's POC. Client will ensure that its POC reviews and acknowledges a list provided by eSentire of eSentire Agent supported operating systems and identifies for eSentire the most critical organizational assets to target for deployment of the Agents. Client acknowledges that the IR Services will require a method of deploying software throughout its organization (e.g., SCCM, PDQDeploy, etc.) and agrees to have a method reasonably satisfactory to eSentire in place prior to commencement of the IR Services. Client is responsible for deploying the Agents in its environment. eSentire will provide up to two hours of support to Client to assist with such deployment at no charge; at Client's request, eSentire will provide additional support at eSentire's then-current hourly rate for such Services. eSentire will install the cloud instance in one availability zone (Amazon data center) selected by Client to support Client's proximity, data residency, and/or privacy requirements. The eSentire Agents will sit in a warm standby state and capture Client data on a rolling 32 consecutive day basis, which can be used in an emergency situation if required. Following expiration of any Contract Year with no subsequent Renewal Term, the Agents will no longer collect data, existing data on the Agents will be deleted, and eSentire will remove the Agents.

1.6 Hourly Rate. The committed hourly rate for Services ordered by Client pursuant to Engagement Letters is detailed on the Order Form. Client may purchase bundles of hours in advance; however, Client will forfeit any previously purchased hours which Client has not used during a given Contract Year.

1.7 Cyber Intelligence. eSentire will provide Client with receive summarized threat intelligence at a cadence determined by eSentire, including customer advisories of known threats. Threat intelligence is not specific to any one customer, but instead is based on relevant threats to the eSentire customer userbase.

1.8 Global Coverage. Agents may be deployed to Client's Windows, macOS, or Linux computing endpoints anywhere in the world, except for embargoed countries, for eSentire to perform fully remote incident response services. For urgent service requests requiring onsite support and ordered pursuant to the processes outlined herein, eSentire may travel throughout the United States and Canada in order to support Client onsite requirements.