GENERAL SERVICES ADMINISTRATION
Federal Supply Service Authorized Federal Supply Schedule Price List

Online access to contract ordering information, terms and conditions, up to date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu database system. The internet address for GSA Advantage!® is: GSAAdvantage.gov.

Multiple Award Schedule (MAS)
Information Technology

7A21: Software Licenses
DB10: Cloud Computing and Cloud Related IT Professional Services
DJ01: Highly Adaptive Cybersecurity Services (HACS)
DA01: Information Technology Professional Services

Contract Number: GS-35F-508CA

Contract Period: September 29, 2015 – September 28, 2025

Pricing Current Through: Modification #PS-0037, signed 09/30/2022

Contractor Name:
Guidepoint Security, LLC
2201 Cooperative Way, Suite 225
Herndon, VA 20171
(877) 889-0132
GSA@guidepointsecurity.com
www.guidepointsecurity.com

Business Size:
Other than small

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at gsa.gov.

Table of Contents

CUSTOMER INFORMATION

1a. Table of awarded special item number(s) with appropriate cross reference to item descriptions and awarded price(s).

SIN	Description
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
54151S	Information Technology Professional Services
511210	Software Licenses
518210C	Cloud Computing and Cloud-Related IT Professional Services
OLM	Order Level Materials

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply. Refer to pricelist as listed herein.

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility, and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate "Not applicable" for this item. Refer to descriptions as listed herein.

2. Maximum Order. $500,000.

3. Minimum Order. $100.00.

4. Geographic coverage (delivery area). 48 contiguous United States and District of Columbia.

5. Point(s) of production (city, county, and State or foreign country). United State for all Guidepoint Security performed services. Production point varies by Manufacturer.

6. Discount from list prices or statement of net price. Prices shown herein are Net (discount deducted).

7. Quantity discounts.

SIN	Quantity Discounts
54151HACS	2% on orders $250,000 or greater.
54151S	2% on orders $250,000 or greater.
511210	None
518210C	2% on orders $250,000 or greater.

8. Prompt payment terms. Note: Prompt payment terms must be followed by the statement "Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions." 0% Net 30 Days.

9. Foreign items (list items by country of origin). Refer to pricelist as listed herein.

10a. Time of delivery. (Contractor insert number of days.)

10b. Expedited Delivery. The Contractor will insert the sentence "Items available for expedited delivery are noted in this price list." under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery. Contract Guidepoint Security, LLC for more information.

10c. Overnight and 2-day delivery. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery. Contract Guidepoint Security, LLC for more information.

10d. Urgent Requirements. The Contractor will note in its price list the "Urgent Requirements" clause of its contract and advise agencies that they can also contact the Contractor's representative to affect a faster delivery. Contract Guidepoint Security, LLC for more information.

11. F.O.B. point(s). Destination

12a. Ordering address(es).

ATTN: Order Processing
Guidepoint Security, LLC
2201 Cooperative Way, Suite 225
Herndon, VA 20171

For order processing assistance: Purchasing@guidepointsecurity.com

12b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs) are found in Federal Acquisition Regulation (FAR) 8.405-3.

13. Payment address(es).

ATTN: Accounts Receivable
Guidepoint Security, LLC
PO Box 742788

Atlanta, GA 30374-2788

For billing assistance: Billing@guidepointsecurity.com

14. Warranty provision. Standard commercial warranty.

15. Export packing charges, if applicable. Not applicable.

16. Terms and conditions of rental, maintenance, and repair (if applicable). Not applicable.

17. Terms and conditions of installation (if applicable). Contract Guidepoint Security, LLC for more information.

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Contract Guidepoint Security, LLC for more information.

18b. Terms and conditions for any other services (if applicable). Contract Guidepoint Security, LLC for more information.

19. List of service and distribution points (if applicable). Contract Guidepoint Security, LLC for more information.

20. List of participating dealers (if applicable). Not applicable.

21. Preventive maintenance (if applicable). Contract Guidepoint Security, LLC for more information.

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). Not applicable.

22b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g., Contractor's website or other location.) The EIT standards can be found at: www.Section508.gov/. Contract Guidepoint Security, LLC for more information.

23. Unique Entity Identifier (UEI) number. JDLCCA1DSVX3

24. Notification regarding registration in System for Award Management (SAM) database. Guidepoint Security, LLC *is* currently registered in the System for Award Management (SAM) database.

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBER 54151HACS)

54151HACS Includes a wide range of fields such as, the seven-step Risk Management Framework services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services and, Security Operations Center (SOC) services. HACS vendors are cataloged under the 5 subcategories of High Value Asset Assessments; Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code: DJ01
Maximum Order: $500,000

NAICS

Number	Description	Business Size
541511	Custom Computer Programming Services	$30 million
541512	Computer Systems Design Services	$30 million
541513	Computer Facilities Management Services	$30 million
541519	Other Computer Related Services	$30 million

Instructions:
Additional SIN Description: Includes proactive and reactive cybersecurity services that improve customer enterprise-level security posture. Services to identify and protect a customer's information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

It encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMA), which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization's incident management functions.

It also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

1. Specific Instructions for SIN 54151HACS - Highly Adaptive Cybersecurity Services (HACS)

a. Offerors may request to be placed in the following subcategories.

i. High Value Asset (HVA) Assessments include Risk and Vulnerability Assessment (RVA) which assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA s individual security components integrate and operate, including how data is protected during operations. Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

ii. Risk and Vulnerability Assessment (RVA) assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

iii. Penetration Testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network.

iv. Incident Response services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state.

v. Cyber Hunt activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.

b. Services offered SIN 54151HACS shall be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M- 19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information
- Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-37 - Risk Management Framework for Information Systems and Organizations: A Systems Life Cycle Approach for Security and Privacy
- NIST SP 800-39 - Managing Information Security Risk: Organization, Mission, and Information System View
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment

- NIST SP 800-128 - Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-160 - Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations.

c. All professional labor categories under SIN 54151S Information Technology Professional Services may remain there, unless the labor categories are specific to SIN 54151HACS.

2. Oral Technical Evaluation for SIN 54151HACS - Highly Adaptive Cybersecurity Services (HACS)

a. Unless otherwise specified, the offeror shall participate in an oral technical evaluation that will be conducted by a Technical Evaluation Board (TEB). The oral technical evaluation will be held at theunclassified level and will be scheduled by the TEB. The oral technical evaluation will be used to assess the offeror's capability to successfully perform the services within the scope of each subcategory as set forth in this solicitation, excepting those service components awarded through the submission of the Service Self-Attestation. The Self-Attestation form is available at gsa.gov/hacs.

An offeror may only be awarded SIN 54151HACS upon successful completion of the Highly Adaptive Cybersecurity Services oral technical evaluation. If the offeror elects to be cataloged under the "Cyber Hunt" and/or "Incident Response" subcategories, additional questions related to those areas will be asked during the HACS Oral Technical Evaluation.

i. ORAL TECHNICAL EVALUATION CONSTRAINTS: The offeror shall identify up to five key personnel, by name and association with the offeror, who will field questions during the oral technical evaluation. The HACS SIN consists of 5 subcategories. The base HACS Oral Technical Evaluation consists of questions related to the 3 subcategories of, High Value Asset Assessments, Risk and Vulnerability Assessments and Penetration Testing. One (1) hour and 40 minutes is allotted for the base HACS Oral Technical Evaluation. The evaluation will be stopped precisely after 1 hour and 40 minutes. Should the offeror elect to be considered for the additional subcategories of Incident Response and Cyber Hunt, an additional 10 minutes will be allotted for each of those

subcategories. The total base evaluation session is expected to last up to 1 hour and 40 minutes, depending on the number of subcategories the offeror is proposing. The TEB Chairperson will be responsible for ensuring the schedule is met and that all offerors are given the same opportunity to present and answer questions.

ii. ORAL TECHNICAL EVALUATION SCHEDULING: The TEB will contact the offeror's authorized negotiator or the signatory of the SF 1449 via email to schedule the oral technical evaluation. Evaluation time slots will be assigned on a first-come-first-served basis. The Government reserves the right to reschedule any offeror's oral technical evaluation at its sole discretion. The oral technical evaluation will be held at facilities designated by the TEB. The exact location, seating capacity, and any other relevant information will be provided when the evaluations are scheduled. The Government may also make accommodations for vendors to participate in the oral evaluations virtually.

iii. PROHIBITION OF ELECTRONIC RECORDING OF THE ORAL TECHNICAL EVALUATION: The offeror may not record or transmit any of the oral evaluation process. All offeror's electronic devices shall be removed from the room during the evaluation. The offeror is permitted to have a timer in the room during the evaluation, provided by the TEB.

iv. RESUBMISSION RESTRICTIONS FOR UNSUCCESSFUL VENDORS UNDER THIS EVALUATION FACTOR: The TEB will afford the offeror multiple opportunities to achieve the "pass" criteria under this evaluation factor through "clarification" questioning, during the Oral Technical Evaluation. Any offeror whom the TEB has found to have not passed under this evaluation factor shall be failed and shall be ineligible to re-submit under the SIN to participate in this evaluation factor for a period of six (6) months following the date of failure.

v. FOR REJECT AND WITHDRAWN OFFERS OR MODIFICATIONS: An offeror or contractor can re-apply for SIN 54151HACS if they are rejected or withdrawn.

1. If an offeror or contractor passes the oral technical evaluation but their offer or modification is rejected or withdrawn, they can re-apply within six (6) months after the oral technical evaluation completion date without having to participate in the oral technical evaluation again. When documentation is resubmitted for review for a new offer/modification, include a statement in the cover letter that the capabilities remain current, accurate, and complete as stated during the oral technical evaluation.

2. If an offeror or contractor passes the oral technical evaluation but their offer or modification is rejected or withdrawn and they do not re-apply within six (6) months after the oral technical evaluation completion date, they must participate in a new oral technical evaluation in order to add SIN 54151HACS.

vi. HIGH VALUE ASSET (HVA) ASSESSMENTS SUBCATEGORY PLACEMENT: Any offeror previously awarded all of the following four SINs: 132-45A Penetration Testing, 132-45B Incident Response, 132-45C Cyber Hunt, and 132-45D Risk and Vulnerability Assessment, shall not be subject to a Highly Adaptive Cybersecurity Services oral technical evaluation, so long as they provide in the modification package to the GSA contracting officer a Service Self-Attestation acknowledging their ability to perform Security Architecture Review (SAR) and Systems Security Engineering (SSE) services in their entirety. The Self-Attestation form is available at gsa.gov/hacs.

b. Oral Technical Evaluation Procedures: The offeror will be evaluated on their knowledge of the proposed services. The oral technical evaluation will require the offeror to respond to a specific scenario and general questions to assess the offeror's expertise. The competencies, criteria and evaluation minimums for the questions are below: All new offerors and modifications must participate in and PASS the HACS Oral Technical Evaluation. The Oral Technical Evaluation will include, at a minimum, questions on Risk and Vulnerability Assessment (RVA), Security Architecture Review (SAR), Systems Security Engineering (SSE), and Penetration Testing. At the time of submission, all new offerors and modifications can also elect to be cataloged in one or both of the additional subcategories of Cyber Hunt or Incident Response (IR). Should this election be taken, additional questions related to these subcategories will be included in their HACS evaluation and these additional subcategory topics must be passed as well.

c. Oral Technical Evaluation Criteria: The offeror's responses to the government's questions during the oral technical evaluation session shall be used to determine whether the offeror has the requisite experience and expertise to perform tasks expected to be performed within the scope of the SIN. The oral technical proposal will be evaluated and rated on a pass/fail basis. The rating definitions provided below will be used for the evaluation of the offeror's responses to questions during the oral evaluation.

d. SIN Subgroups: Upon completion of the oral technical evaluation for both offers and modifications, the government will determine which of the following 5 SIN subgroups apply:

1. High value Asset (HVA) Assessments
2. Risk and Vulnerability Assessment (RVA)

3. Cyber Hunt
4. Incident Response
5. Penetration Testing

Following notification that they are eligible for one or more of the 5 SIN subgroups, awarded contractors may select the corresponding subgroups by following the instructions below:

1. Login to eBuy
2. From the top menu, select "Profile"
3. Click "Modify Subgroups"
4. Select the applicable subgroups according to the instructions

All contractor selections will be monitored by GSA for compliance and action will be taken against your contract if you select Subgroups that have not been awarded under your contract.

Note: All services shall be billed in arrears in accordance with 31 U.S.C. 3324.

TECHNICAL RATINGS	
Rating	**Definition**
Pass	The proposal clearly meets the minimum requirements of the solicitation.
Fail	The proposal does not clearly meet the minimum requirements of the solicitation.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

54151S IT Professional Services and/or labor categories for database planning and design; systems analysis, integration, and design; programming, conversion, and implementation support; network services, data/records management, and testing.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code: DA01
Maximum Order: $500,000

NAICS

Number	Description	Business Size
541511	Custom Computer Programming Services	$30 million
541512	Computer Systems Design Services	$30 million
541513	Computer Facilities Management Services	$30 million
541519	Other Computer Related Services	$30 million

Instructions:

1. Specific Instructions for SIN 54151S - Information Technology Professional Services:

* All services shall be billed in arrears in accordance with 31 U.S.C. 3324.

TERMS AND CONDITIONS APPLICABLE TO SOFTWARE LICENSES (SPECIAL ITEM NUMBER 511210)

511210 Includes both term and perpetual software licenses and maintenance. Includes operating system software, application software, EDI translation and mapping software, enabled email message based applications, Internet software, database management applications, and other software.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code: 7A21
Maximum Order: $500,000

NAICS

Number	Description	Business Size
511210	Software Publishers	$41.5 million

Instructions:
Additional SIN Description: Term Licenses. The word "Term" is defined in this Solicitation as "a limited period of time". Term Software Licenses have a limited duration and are not owned in perpetuity. Unless Offerors provide an option for converting Term licenses into perpetual licenses, users lose the right to use these licenses upon the end of the term period. This SIN is NOT Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS) as defined in SIN 518210C - Cloud Computing and Cloud Related IT Professional Services. Term Software Licenses are distinct from Electronic Commerce and Subscription Services (SIN 54151ECOM).

Perpetual Licenses The word "perpetual" is defined in this Solicitation as "continuing forever, everlasting, valid for all time".

Software maintenance as a product includes the publishing of bug/defect fixes via patches and updates/upgrades in function and technology to maintain the operability and usability of the software product. It may also include other no charge support that is included in the purchase price of the product in the commercial marketplace. No charge support includes items such as user blogs, discussion forums, online help libraries and FAQs (Frequently Asked Questions), hosted chat rooms, and limited telephone, email and/or web-based general technical support for users self diagnostics.

Software Maintenance as a product is billed at the time of purchase.

Software maintenance as a product does NOT include the creation, design, implementation, integration, etc. of a software package. These examples are considered software maintenance services under SIN 54151 Software Maintenance Services.

1.) Specific Instructions for SIN 511210 - Software Licenses

a.) Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at http://www.core.gov.

b.) The words “term software” or “perpetual software” shall be the first word in the product title/name for: 1) the price proposal template and 2) the SIP file for GSA Advantage. The word “term software” or “perpetual software” shall be the first word in the product title/name for the GSA Pricelist pricing charts (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016). The words “term software” or “perpetual software” shall be in each product title in any response to a customer Request for Quote (RFQ) or Request for Information (RFI).

c.) Contractors are encouraged to offer SIN 54151 Software Maintenance Services in conjunction with SIN 511210 - Software Licenses.

d.) Conversion From Term License To Perpetual License

i.) When standard commercial practice offers conversions of term licenses to perpetual licenses, and an ordering activity requests such a conversion, the contractor shall provide the total amount of conversion credits available for the subject software within ten (10) calendar days after placing the order.

ii.) When conversion credits are provided, they shall continue to accrue from one contract period to the next, provided the software has been continually licensed without interruption.

iii.) The term license for each software product shall be discontinued on the day immediately preceding the effective date of conversion from a term license to a perpetual license.

iv.) When conversion from term licenses to perpetual licenses is offered, the price the ordering activity shall pay will be the perpetual license price that prevailed at the time such software was initially ordered under a term license, or the perpetual license price prevailing at the time of conversion from a term license to a perpetual license, whichever is the less, minus an amount equal to a percentage of all term license payments during the period that the software was under a term license within the ordering activity.

e.) Term License Cessation

i.) After a software product has been on a continuous term license for a period of _____ (Fill-in the period of time.) months, a fully paid-up, non-exclusive, perpetual license for the software product shall automatically accrue to the ordering activity. The period of continuous term license for automatic accrual of a fully paid-up perpetual license does not have to be achieved during a particular fiscal year; it is a written Contractor commitment which continues to be available for software that is initially ordered under this contract, until a fully paid-up perpetual license accrues to the ordering activity. However, should the term license of the software be discontinued before the specified period of the continuous term license has been satisfied, the perpetual license accrual shall be forfeited. Contractors who do not commercially offer conversions of term licenses to perpetual licenses shall indicate that their term licenses are not eligible for conversion at any time.

ii.) Each separately priced software product shall be individually enumerated, if different accrual periods apply for the purpose of perpetual license attainment.

iii.) Fill-in data and specific terms shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016)).

iv.) The Contractor agrees to provide updates and software maintenance services for the software after a perpetual license has accrued, at the prices and terms of SIN 54151 – Software Maintenance Services, if the licensee elects to order such services. Title to the software shall remain with the Contractor.

f.) Utilization Limitations for Perpetual Licenses

i.) Software Asset Identification Tags (SWID) (Option 1 Perpetual License)

1.) Option 1 is applicable when the Offeror agrees to include the International Organization for Standardization/International Electrotechnical Commission 19770-2 (ISO/IEC 19770- 2:2015) standard identification tag (SWID Tag) as an embedded element in the software. An ISO/IEC 19970-2 tag is a discoverable identification element in software that provides licensees enhanced asset visibility. Enhance visibility supports both the goals of better software asset management and license compliance. Offerors may use the National Institute of Standards and Technology (NIST) document “NISTIR 8060: Guidelines for Creation of Interoperable Software Identification (SWID) Tags,” December 2015 to determine if they are in compliance with the ISO/IEC 19770-2 standard.

2.) Section 837 of The Federal Information Technology Acquisition Reform Act (FITARA) of 2014, requires GSA to seek agreements with software vendors that enhance government- wide acquisition, shared use, and dissemination of software, as well as compliance with end user license agreements. The Megabyte Act of 2016 requires agencies to inventory software assets and to make informed decisions prior to new software acquisitions. In June of 2016, the Office of Management and Budget issued guidance on software asset management requiring each CFO Act (Public Law 101-576 – 11/15/1990) agency to begin software inventory management (M-16-12). To support these requirements, Offerors may elect to include the terms of Option 1 and/or Option 2, which support software asset management and government-wide reallocation or transferability of perpetually licensed software.

ii.) Reallocation of Perpetual Software (Option 2 Perpetual License)

1.) The purpose of SIN 511210 OPTION 2 is to allow ordering activities to transfer software assets for a pre-negotiated charge to other ordering activities.

2.) When an ordering activity becomes aware that a reusable software asset may be available for transfer, it shall contact the Contractor, identify the software license or licenses in question, and request that these licenses be reallocated or otherwise made available to the new ordering activity.

3.) Contractors shall release the original ordering activity from all future obligations under the original license agreement and shall present the new ordering activity with an equivalent license agreement. When the new ordering activity agrees to the license terms, henceforth any subsequent infringement or breach of licensing obligations by the new ordering activity shall be a matter exclusively between the new ordering activity and the Contractor.

4.) The original ordering activity shall de-install, and/or make unusable all of the software assets that are to be transferred. It shall have no continuing right to use the software and any usage shall be considered a breach of the Contractor's intellectual property and a matter of dispute between the original ordering activity/original license grantee and the licensor.

5.) As a matter of convenience, once the original licenses are deactivated, di-installed, or made otherwise unusable by the original ordering activity or license grantee, the Contractor may elect to issue new licenses to the new ordering activity to replace the old licenses. When new licenses are not issued, the Contractor shall provide technical advice on how best to achieve the functional transfer of the software assets.

6.) Software assets that are eligible for transfer that have lapsed Software Maintenance Services (SIN 54151) may require a maintenance reinstatement fee, chargeable to the new ordering activity or license grantee. When such a fee is paid, the new ordering activity shall receive all the rights and benefits of Software Maintenance Services.

7.) When software assets are eligible for transfer, and are fully covered under pre-paid Software Maintenance Services (SIN 54151), the new ordering activity shall not be required to pay maintenance for those license assets prior to the natural termination of the paid for maintenance period. The rights associated with paid for current Software Maintenance Services shall automatically transfer with the software licenses without fee. When the maintenance period expires, the new ordering activity or license grantee shall have the option to renew maintenance.

8.) The administrative fee to support the transfer of licenses, exclusive of any new incremental licensing or maintenance costs shall be _____ percentage (%) of the original license fee. The fee shall be paid only at the time of transfer. In applying the transfer fee, the Software Contractor shall provide transactional data that supports the original costs of the licenses.

9.) Fill-in data and specific terms shall be attached to the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016).

g.) Software Conversions: Full monetary credit will be allowed to the ordering activity when conversion from one version of the software to another is made as a result of a change in operating system, or from one computer system to another. Under a perpetual license, the purchase price of the new software shall be reduced by the amount that was paid to purchase the earlier version. Under a term license, if conversion credits had accrued while the earlier version was under a term license, those credits shall carry forward and remain available as conversion credits which may be applied towards the perpetual license price of the new version.

TERMS AND CONDITIONS APPLICABLE TO CLOUD COMPUTING AND CLOUD RELATED IT PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 518210C)

518210C Includes commercially available cloud computing services such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and emerging cloud computing services. IT professional services that are focused on providing the types of services that support the Government's adoption of, migration to, or governance/management of cloud computing. Specific cloud related IT professional labor categories and/or fixed-price professional services solutions (e.g., migration services) that support activities associated with assessing cloud solutions, refactoring workloads for cloud solutions, migrating legacy or other systems to cloud solutions, providing management/governance of cloud solutions, DevOps, developing cloud native applications, or other cloud oriented activities are within scope of this SIN.

NOTE: Subject to Cooperative Purchasing

Cooperative Purchasing: Yes
Set Aside: No
FSC/PSC Code: DB10
Maximum Order: $500,000

NAICS

Number	Description	Business Size
518210	Data Processing, Hosting, and Related Services	$35 million

Instructions:
Additional SIN Description: This SIN provides access to cloud (e.g., IaaS, PaaS, SaaS) computing services across public, community, and hybrid deployment models. Cloud computing services shall comply with National Institute of Standards and Technology (NIST) Definition of Cloud Computing Essential Characteristics (NIST SP 800-145). Cloud computing that does not meet all NIST essential characteristics are outside the scope of this SIN and shall be assigned to other SINs, where applicable.

Cloud related IT professional labor categories are within scope of this SIN. Cloud related IT professional labor categories are not subject to adherence to the NIST definition of cloud computing; therefore, no technical response is required for a labor proposal. Non-professional labor categories subject to Service Contract Labor Standards (SCLS) (e.g., IT help desk support) that are incidental to and used solely to support specific Cloud related IT professional labor categories and/or fixed-price professional services solutions must be offered under a different SIN that specifically covers the proposed services.

Ancillary products and services are not within scope of this SIN. Any items that are not within the scope of this SIN must be offered under a SIN that specifically covers the proposed services.

The following are out of scope for this SIN: cloud "token," "gift card," "credit," or other similar types of prepaid offerings:

1.) Cloud computing services (e.g., IaaS, PaaS, SaaS) are sometimes offered commercially as a cloud "token," "gift card," "credit," or require purchase of a prepaid offering; these are out of scope for this SIN. The pricing model for these items do not accurately represent the stock-keeping units (SKU) that are awarded at the task-order level. Therefore, nonsubmission of pricing of underlying IaaS, PaaS, SaaS SKUs is not allowed.

2.) Credits for cloud computing services (e.g., IaaS, PaaS, SaaS) that are paid for in advance and spent or used at a later time are commonly termed commercially as a cloud "token," "gift card," or "credit", and are out of scope for SIN 518210C. Cloud computing services (e.g., IaaS, PaaS, SaaS) must be paid for in arrears in accordance with 31 U.S.C. 3324.

3.) Also out of scope is any payment for cloud computing services which carry a risk to the Government of a "use or lose" situation where a Government cloud account may forfeit unexpended credits/deposits towards future cloud computing services charges at the end of a vendor-defined period (e.g., 1, 2 or 3 years). Therefore, pre-payment of products or services prior to delivery of SKUs is not allowed. Payment for these SKUs must be in arrears.

Physical hardware, non-cloud software per the NIST definition, and other artifacts acquired to support the physical construction of a private or other cloud are not within the scope of this SIN.

1) Specific Instructions for SIN 518210C – Cloud Computing and Cloud Related IT Professional Services

a) All offerings must be billed as follows:

i) Cloud computing services (e.g., IaaS, PaaS, SaaS) must adhere to the "pay as you go" pricing model and must be billed in arrears in accordance with 31 U.S.C. 3324.

ii) Cloud related IT professional services, specific cloud labor categories and/or fixed-price professional services solutions must also be billed in arrears in accordance with 31 U.S.C. 3324.

b) Offerors shall follow instructions and guidance for cloud computing services available at http://www.gsa.gov/mascategoryrequirements

c) Offerors may propose:

i) Cloud computing services only (e.g., IaaS, PaaS, SaaS);

ii) Cloud related IT professional services and/or fixed-price professional services solutions that are not subject to NIST standards only; or

iii) Cloud computing services (e.g., IaaS, PaaS, SaaS) (subject to NIST standards) and cloud related IT professional services and/or fixed-price professional services solutions (not subject to NIST standards).

iv) The offeror must state which cloud computing service model(s), if any, is/are being proposed (e.g., IaaS, PaaS, SaaS).

v) The offeror must state which cloud computing deployment model(s), if any, is/are being proposed (e.g., public, community, and hybrid).

d) Acceptance Testing: Acceptance testing shall be performed of the systems for ordering activity approval in accordance with the approved test procedures.

e) Training

i) If training is provided in accordance with standard commercial practices, the offeror shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system.

ii) If there are separate training charges, they should be included in the GSA Price List (I-FSS-600 CONTRACT PRICE LISTS (OCT 2016).

f) Information Assurance/Security Requirements: Offerors shall meet information assurance/security requirements in accordance with the ordering activity requirements.

g) Reporting: Offerors shall provide to the ordering activity any general reporting capabilities available to verify performance, cost and availability. In accordance with commercial standard practice, the offeror may furnish the ordering activity with a monthly summary report.

h) Cloud related IT professional services may be listed on SIN 54151S - Information Technology Professional Services. The cloud related IT professional services on this SIN (518210C) shall be cloud specific titles and descriptions. At a minimum, the word “cloud” shall appear both in the title and the description of each labor category or fixed-price professional services solutions proposed for this SIN. The relevant past performance projects must demonstrate that the cloud related IT professional services were utilized in the IaaS, PaaS, and/or SaaS environment. NOTE: Identical labor categories cannot be on both SINs 54151S and 518210C. It is recommended that cloud

related IT professional services and/or fixed-price professional services solutions that are not subject to NIST standards should be offered under SIN 518210C.

i) Offerors may optionally select a single service model that best fits a proposed cloud computing offering. Only one service model may be selected per each proposed cloud computing offering. Offerors may elect to submit multiple cloud computing offerings, each with its own single service model.

j) Deployment model selection within this SIN is optional for any individual cloud computing offering. Offerings may be included without a deployment model selection so long as they comply with all the essential characteristics of cloud computing as outlined by NIST SP 800-145. The three NIST deployment models within the scope of this SIN are: Public, Community, and Hybrid.

k) All current pricing requirements in provision SCP-FSS-001 apply. At the current time, there is no provision for reducing or eliminating standard price list posting requirements to accommodate rapid cloud price fluctuations.

l) All pricing models for cloud computing services must have the core capability to meet the NIST Essential Cloud Characteristics, particularly with respect to on-demand self-service, while allowing alternate variations at the task order level at agency discretion, pursuant to the guidance on NIST Essential Characteristics.

m) Evaluation factors for cloud related IT professional services, specific cloud labor categories and/or fixed-price professional services solutions are found within this same document under Section II Instructions for all IT Offerors under 6) Relevant Project Experience Evaluation.

2) Specific Evaluation Factor for Cloud Computing Services Adherence to the NIST Essential Cloud Characteristics per NIST SP 800-145.

Within a two-page limitation for each cloud computing service (e.g., IaaS, PaaS, SaaS) submitted, provide a description of how the cloud computing service meets each of the five essential cloud computing characteristics as defined in National Institute of Standards and Technology (NIST) Special Publication 800-145 and subsequent versions of this publication. This standard specifies the definition of cloud computing for use by Federal agencies. Each cloud computing service must be capable of satisfying each of the five NIST essential characteristics as follows:

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity

- Measured service cloud (Pay per use, or pay as you go)

Refer to 518210C. Specific Information for Offerors available at http://www.gsa.gov/mascategoryrequirements for guidance on meeting the NIST essential characteristics. For the purposes of the cloud computing and cloud related IT professional services SIN, meeting the NIST essential characteristics is concerned primarily with whether the underlying capability of the commercial service is available, and whether or not an ordering activity actually requests or implements the capability.

ALLOWABLE SUBSTITUTIONS OF EDUCATION AND EXPERIENCE (APPLICABLE TO SINS 54151HACS, 54151S, AND 518210C)

The minimum education and experience will be met when the equivalencies in the tables below are considered.

Additional educational achievements greater than the requirements can be substituted for experience requirements:

Required Education	Actual Education	Additional Years of Experience Credited to the Employee
BA/BS	Ph.D.	4
BA/BS	MA/MS	2

Due to the availability or limitation of education, occasionally substitution of experience as referenced below for a professional labor type with additional years of experience in an Information Technology related field will be provided per the approval of the federal agency acquiring the service:

Actual Education	Required Education	Additional Years of Experience Needed for Educational Requirements Equivalency
High School/GED	BA/BS	4
AA/AS	BA/BS	2
Professional Certification(s) in the related Information Technology field	BA/BS	2

LABOR CATEGORY DESCRIPTIONS AND PRICING (SINs 54151HACS, 54151S and 518210C)

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
54151S	**Senior Subject Matter Expert**	**Duties:** Confers with client management and leads in the outline and development of a client's strategic information security and information technology business goals and IT strategy. Analyzes client requirements and recommends development or acquisition strategies. Assists clients in developing strategic plans and concepts. Advises client on the impact of new legislation or new technologies that are relevant to their agency. Demonstrates exceptional oral and written communication skills. Possesses requisite knowledge and expertise so recognized in the professional community that the individual is considered "expert" in the technical/specialty area being addressed. **Education/Experience:** BA/BS and 12 years of experience	$253.90
54151S	**Subject Matter Expert**	**Duties:** Provides insight and guidance to the client regarding their strategic information security and information technology business goals and IT strategy. Analyzes client requirements and recommends development or acquisition strategies. Assists clients in developing strategic plans and concepts. Advises client on the impact of new legislation or new technologies that are relevant to their agency. Demonstrates exceptional oral and written communication skills. Possesses requisite knowledge and expertise so recognized in the professional community that the individual is considered "expert" in the technical/specialty area being addressed. **Education/Experience:** BA/BS and 10 years of experience.	$199.94
54151S	**Project Manager**	**Duties:** Plans and directs a highly technical project (or a group of related tasks) and assists	$172.29

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		in working with the government Contracting Officer, the COTR, government management personnel, and client agency representatives. Under the guidance of the client representative, is responsible for the overall management of specific Task Orders and ensures that the technical solutions and schedules in the Task Order are implemented in a timely manner. **Education/Experience:** BA/BS and 10 years of experience.	
54151S	**Managing Security Consultant**	**Duties:** Directs the consulting teams in the delivery of information security, information security systems, and/or computer security requirements. Designs, develops, engineers, and implements security solutions. Gathers and organizes technical information about an organization's mission, goals, and needs; existing security products; and ongoing programs. Develops, analyzes, and implements security architecture(s) as appropriate. Performs risk analysis and security audit services, develops analytical reports as required. May be required to perform in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery, incident response, application assessment, vulnerability threat management, cloud security, and contingency planning; telecommunications security; development of security policies and procedures. May be responsible for leading a team in performing these services. **Education/Experience:** BA/BS and 10 years of experience.	$181.36
54151S	**Senior Security Consultant**	**Duties:** Analyzes and defines security requirements and designs, develops, engineers, and implements solutions. Performs risk analysis and security audit services, developing analytical	$163.22

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		reports as required. May be required to perform in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery and contingency planning; telecommunications security; development of security policies and procedures. **Education/Experience:** BA/BS and 3 years of experience.	
54151S	**Security Consultant**	**Duties:** Assists more experienced consultants in analyzing and defining security requirements. Assists in performing risk analysis and security audit services and in developing analytical reports. May assist in performing in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery and contingency planning; telecommunications security; development of security policies and procedures. **Education/Experience:** BA/BS and 2 years of experience.	$154.16
54151S	**Security Analyst**	**Duties:** Assisting member of a team for delivering on a specific task of a small/simple projects individually and large projects as a team member with oversight and continual skill development. **Education/Experience:** BA/BS and 0 to 2 years of experience.	$149.62
54151S	**Managing Security Engineer**	**Duties:** Directs the engineering teams in the delivery of information security product solutions, information security systems, and/or computer security requirements. Designs, develops, engineers, and implements security solutions. Gathers and organizes technical information about an organization's mission, goals, and needs; existing security products; and	$181.36

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		ongoing programs. Develops, analyzes, and implements security architecture(s) as appropriate. Performs risk analysis and security audit services, develops analytical reports as required. May be required to perform in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery, incident response, application assessment, vulnerability threat management, cloud security, and contingency planning; telecommunications security; development of security policies and procedures. May be responsible for leading a team in performing these services. **Education/Experience:** BA/BS and 10 years of experience.	
54151S	**Senior Security Architect**	**Duties:** Responsible for the analysis, development, and design of the enterprise information architecture by determining security requirements; planning, implementing, and testing security systems; preparing security standards, policies, and procedures; mentoring team members. **Education/Experience:** BA/BS and 5 years of experience.	$167.76
54151S	**Senior Security Engineer**	**Duties:** Engineering technical lead of security solutions through analysis, requirement assessment, network designs, through solution implementation. Leads the engineer team with complex integration and implementation of network security stack-based devices. Performs risk analysis and security audit services, developing analytical reports as required. Directs the team in performing in one or more of the following areas: analysis & design; implementation; optimization; security of computer hardware; operating system utility/support software; disaster recovery and	$163.22

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		contingency planning; telecommunications security; development of security policies and procedures. **Education/Experience:** BA/BS and 3 years of experience.	
54151S	**Security Engineer**	**Duties:** Assists more experienced engineers in the implementation and optimization of IT infrastructure security solutions. Assists in performing the engineers with complex integration and implementation of network security stack-based devices. May assist in performing in one or more of the following areas: analysis & design; implementation; optimization; security of computer hardware; operating system utility/support software; disaster recovery and contingency planning; telecommunications security; development of security policies and procedures. **Education/Experience:** BA/BS and 0 to 2 years of experience.	$149.62
54151HACS	**Senior Subject Matter Expert**	**Duties:** Confers with client's senior security management team and leads in the outline and development of a client 's strategic Information Assurance systems plans, information security technology business goals and the client's cybersecurity management strategy. Analyzes and assesses client cybersecurity systems and architecture requirements and recommends development or acquisition strategies for security solutions. Assists clients in developing strategic cybersecurity plans and concepts. Advises client on the impact of new cybersecurity legislation, mandates, regulations, or new technologies and industry best-practices that are relevant to their agency. Demonstrates exceptional oral and written communication skills. Possesses requisite knowledge and expertise so recognized in the professional cybersecurity community that the individual is	$253.90

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		considered "expert" in the Information Assurance area being addressed. **Education/Experience:** BA/BS and 12 years of experience	
54151HACS	**Subject Matter Expert**	**Duties:** Provides insight and guidance to the client regarding their strategic Information Assurance systems plans, information security technology business goals and the client's cybersecurity management strategy. Analyzes and assesses client cybersecurity systems and architecture requirements and recommends development or acquisition strategies for security solutions. Assists clients in developing strategic cybersecurity plans and concepts. Advises client on the impact of new cybersecurity legislation, mandates, regulations or new technologies and industry best-practices that are relevant to their agency. Demonstrates superior oral and written communication skills. Possesses requisite knowledge and expertise so recognized in the professional cybersecurity community that the individual is considered "expert" in the Information Assurance area being addressed. **Education/Experience:** BA/BS and 10 years of experience.	$199.94
54151HACS	**Project Manager**	**Duties:** Plans and directs Information Assurance programs or projects (or a group of related Cybersecurity tasks) and assists in working with the government Contracting Officer, the COTR, government management personnel (CISO, ISSM), and client security representatives. Under the guidance of the client representative, is responsible for the overall management of specific security-based Task Orders and ensures that the Information Assurance security solutions and schedules in the Task Order are implemented in a timely manner. **Education/Experience:** BA/BS and 10 years of experience.	$172.29

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
54151HACS	**Managing Security Consultant**	**Duties:** Directs the Cybersecurity and IA teams in the delivery of information security, information security systems, and/or computer security requirements. Architects, assesses, develops, engineers, and implements Cybersecurity solutions. Retrieves, gathers, and organizes technical information about an organization's risks, vulnerabilities, and exposures within the existing security products, networks, applications, and programs. Develops, analyzes, and implements Cybersecurity architecture(s) as appropriate. Performs risk analysis assessments, conducts Cybersecurity governance and compliance services, develops analytical and technical reports as required. May be required to perform in one or more of the following areas: risk and vulnerability assessments; cyber hunting activities; conducting penetration testing and scanning; assessment of system security for compliance; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures. May be responsible for leading a team in performing these services. **Education/Experience:** BA/BS and 10 years of experience.	$181.36
54151HACS	**Senior Security Consultant**	**Duties:** Analyzes and defines security requirements and designs, develops, engineers, and implements solutions. Performs risk analysis and security audit services, developing analytical reports as required. May be required to perform in one or more of the following areas: risk and vulnerability assessments; cyber hunting activities; conducting penetration testing and scanning; assessment of system security for	$163.22

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		compliance; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures. **Education/Experience:** BA/BS and 3 years of experience.	
54151HACS	**Security Consultant**	**Duties:** Assists more experienced consultants in analyzing and defining security requirements. Assists in performing risk analysis and security audit services and in developing analytical reports. May assist in performing in one or more of the following areas: Risk and Vulnerability Assessments; Cyber Hunting activities; conducting Penetration Testing and scanning; assessment of system security for compliance of applications; security of computer network hardware; operating system utility/support software; disaster recovery; incident response and digital forensics; application assessment; vulnerability threat management; cloud security; contingency planning; social engineering; and the development of security policies and procedures. **Education/Experience:** BA/BS and 2 years of experience.	$154.16
54151HACS	**Security Analyst**	**Duties:** Assisting member of a team for delivering on a specific Cybersecurity task of a small/simple projects individually and large projects as a team member with oversight and continual skill development. **Education/Experience:** BA/BS and 0 to 2 years of experience.	$149.62
518210C	**Cloud Security Consultant**	**Duties:** Assists more experienced consultants in analyzing and defining cloud security requirements. Assists in performing risk analysis and security audit services and in developing	$180.76

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		analytical reports. May assist in performing in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery, incident response, application assessment, vulnerability threat management, cloud security, penetration testing and contingency planning; support the development of security policies and procedures. **Education/Experience:** BA/BS and 2 years of experience.	
518210C	**Cloud Senior Security Consultant**	**Duties:** Analyzes and defines cloud security requirements and designs, develops, engineers, and implements solutions. Performs risk analysis and security audit services, developing analytical reports as required. May be required to perform in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery, incident response, application assessment, vulnerability threat management, cloud security, penetration testing and contingency planning; development of security policies and procedures. May be responsible for leading a team in performing these services. **Education/Experience:** BA/BS and 3 years of experience.	$194.66
518210C	**Cloud Managing Security Consultant**	**Duties:** Directs the consulting teams in the delivery of cloud information security, cloud information security systems, and/or cloud computer security requirements. Designs, develops, engineers, and implements security solutions. Gathers and organizes technical information about an organization's mission, goals, and needs; existing security products; and ongoing programs. Develops, analyzes, and	$208.56

SIN	Labor Category Title	Position Description	GSA Price (Hourly)
		implements cloud security architecture(s) as appropriate. Performs risk analysis and security audit services, develops analytical reports as required. May be required to perform in one or more of the following areas: risk assessment methods and procedures; security of system software generation; security of computer hardware; operating system utility/support software; disaster recovery, incident response, application assessment, vulnerability threat management, cloud security, penetration testing, and contingency planning; telecommunications security; development of security policies and procedures. Responsible for leading a team in performing these services. **Education/Experience:** BA/BS and 5 years of experience.	
518210C	**Cloud Senior Security Architect**	**Duties:** Responsible for the analysis, development, and design of the cloud enterprise information architecture by determining security requirements; planning, implementing, and testing security systems; preparing security standards, policies, and procedures; mentoring team members. **Education/Experience:** BA/BS and 5 years of experience.	$231.74
518210C	**Cloud Project Manager**	**Duties:** Coordinates resources to a cloud technical project or portions of a technical Program to manage deliverables, burn rate, and other task related across a specific project, Work with the government Contracting Officer, the COTR, government management personnel, and client agency representatives. Under the guidance of the client representative, is responsible for the coordination of a specific project and ensures that the technical solutions and schedules in the project are implemented in a timely manner. **Education/Experience:** BA/BS and 2 years of experience.	$180.76

GUIDEPOINT SECURITY SERVICE OFFERINGS AND PRICING

The SIN quantity/volume discount does not apply to the service offerings listed hereunder

SIN	Service Offering Title	Service Offering Description	GSA Price
54151S	**GuidePoint SOAR Services-Standard**	GuidePoint Security will provide services for your SOAR platform. This service includes, but is not limited to, standard configuration of your SOAR platform, and basic playbook development and integrating products into workflow actions. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,632.24
54151S	**GuidePoint SOAR Services-Remote**	GuidePoint Security will provide services for your SOAR platform. This service includes, but is not limited to, standard configuration of your SOAR platform, and basic playbook development and integrating products into workflow actions. Such services will be provided remotely. ***Price is daily*** during normal hours of business.	$1,450.88
54151S	**GuidePoint SOAR Services-Premium**	GuidePoint Security will provide premium services for your SOAR platform that require extensive SOAR expertise. This service offering includes, but is not limited to, tasks such as assisting with platform selection based on your requirements, architecture & design, reviewing SOC workflows and creating a SOAR implementation plan that includes a sustainable foundation for your SOAR environment. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,813.60
54151S	**GuidePoint Splunk Services-Standard**	GuidePoint Security will provide services for Splunk core infrastructure, architecture and design, installation, data collection, log governance, and onboarding and management, and ensuring best practices across the entire Splunk lifecycle are addressed. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,632.24

SIN	Service Offering Title	Service Offering Description	GSA Price
54151S	**GuidePoint Splunk Services-Remote**	GuidePoint Security will provide services for Splunk core infrastructure, architecture and design, installation, data collection, log governance, and onboarding and management, and ensuring best practices across the entire Splunk lifecycle are addressed. Such services will be provided remotely. ***Price is daily*** during normal hours of business.	$1,450.88
54151S	**GuidePoint Splunk Services-Premium**	Guidepoint Security will provide services for Splunk environments that involve their premium applications. GuidePoint will assist with products such as Enterprise Security, ITSI, and UBA. These services include, but is not limited to, architecture and design, installation, configuration, optimizing & tuning, and creating specific use case content for Splunk Premium Applications. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,813.60
54151S	**GuidePoint F5 Networks Services-Standard**	GuidePoint Security will provide services for an F5 solution that includes standard F5 features. This service offering includes, but is not limited to, tasks such as architecting and configuring F5 LTM, F5 DNS (Previously known as GTM), F5 APM (Basic/Simple deployments), F5 AFM, BIG-IQ, F5 AWAF (Basic/Simple deployments) implementation and standard O&M of your base F5 platform. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,632.24
54151S	**GuidePoint F5 Networks Services-Remote**	GuidePoint Security will provide services for an F5 solution that includes standard F5 features. This service offering includes, but is not limited to, tasks such as architecting and configuring F5 LTM, F5 DNS (Previously known as GTM), F5 APM (Basic/Simple deployments), F5 AFM, BIG-IQ, F5 AWAF (Basic/Simple deployments) implementation and standard O&M of your base F5 platform. Such services will be provided remotely. ***Price is daily*** during normal hours of business.	$1,450.88

SIN	Service Offering Title	Service Offering Description	GSA Price
54151S	**GuidePoint F5 Networks Services-Premium**	GuidePoint Security will provide premium professional services for an F5 solution that includes premium F5 features. This service offering includes, but is not limited to, tasks such as advanced architecting and configuring of SSL Orchestration, F5 AWAF, F5 APM, F5 AFM, and other F5 modules. Such services are on-site. ***Price is daily*** during normal hours of business.	$1,813.60
54151HACS	**Threat & Attack Simulation Services - External Penetration Testing - 20 or fewer live hosts.**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$11,047.86
54151HACS	**Threat & Attack Simulation Services - External Penetration Testing - 21 to 50 live hosts.**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$14,109.57
54151HACS	**Threat & Attack Simulation Services - External Penetration Testing - 51 to 100 live hosts.**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$22,823.68
54151HACS	**Threat & Attack Simulation Services - External Penetration**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on	$38,367.76

SIN	Service Offering Title	Service Offering Description	GSA Price
	Testing - 101 to 400 live hosts.	customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	
54151HACS	**Threat & Attack Simulation Services - External Penetration Testing - 401 to 800 live hosts.**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$55,068.01
54151HACS	**Threat & Attack Simulation Services - External Penetration Testing - 801 to 1200 live hosts.**	Guidepoint to conduct an External Penetration Test, performed from the perspective of an attacker on the Internet in an attempt to find weak areas of customer's perimeter network. Guidepoint will also perform reconnaissance on customer to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$72,496.22
54151HACS	**Threat & Attack Simulation Services - Internal Penetration Testing - 500 or fewer live hosts.**	Guidepoint to conduct a penetration test of customer's internal environment, simulating an attacker on the internal network, and will actively exploit vulnerabilities to provide a tangible demonstration of the impact of unpatched vulnerabilities and secure configuration deficiencies in clear, repeatable steps. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$18,819.90
54151HACS	**Threat & Attack Simulation Services - Internal Penetration Testing - 501 to 1500 live hosts.**	Guidepoint to conduct a penetration test of customer's internal environment, simulating an attacker on the internal network, and will actively exploit vulnerabilities to provide a tangible demonstration of the impact of unpatched vulnerabilities and secure configuration deficiencies in clear, repeatable steps. The engagement will evaluate the scope,	$28,005.04

SIN	Service Offering Title	Service Offering Description	GSA Price
		security, and resiliency of customer's environment.	
54151HACS	**Threat & Attack Simulation Services - Internal Penetration Testing - 1501 to 4000 live hosts.**	Guidepoint to conduct a penetration test of customer's internal environment, simulating an attacker on the internal network, and will actively exploit vulnerabilities to provide a tangible demonstration of the impact of unpatched vulnerabilities and secure configuration deficiencies in clear, repeatable steps. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$44,255.67
54151HACS	**Threat & Attack Simulation Services - Internal Penetration Testing - 4000+ live hosts.**	Guidepoint to conduct a penetration test of customer's internal environment, simulating an attacker on the internal network, and will actively exploit vulnerabilities to provide a tangible demonstration of the impact of unpatched vulnerabilities and secure configuration deficiencies in clear, repeatable steps. The engagement will evaluate the scope, security, and resiliency of customer's environment.	$57,658.69
54151HACS	**Threat & Attack Simulation Services - External Network Vulnerability Assessment - 5 or fewer external live hosts.**	Guidepoint to conduct an External Vulnerability Assessment of Client's external (Internet-facing) environment to identify vulnerabilities and weaknesses within its external environment. GuidePoint also will perform reconnaissance on Client to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of Client's environment.	$2,098.24
54151HACS	**Threat & Attack Simulation Services - External Network Vulnerability Assessment - 6 to 20 external live hosts.**	Guidepoint to conduct an External Vulnerability Assessment of Client's external (Internet-facing) environment to identify vulnerabilities and weaknesses within its external environment. GuidePoint also will perform reconnaissance on Client to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of Client's environment.	$4,217.88

SIN	Service Offering Title	Service Offering Description	GSA Price
54151HACS	**Threat & Attack Simulation Services - External Network Vulnerability Assessment - 21 to 50 external live hosts.**	Guidepoint to conduct an External Vulnerability Assessment of Client's external (Internet-facing) environment to identify vulnerabilities and weaknesses within its external environment. GuidePoint also will perform reconnaissance on Client to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of Client's environment.	$6,573.05
54151HACS	**Threat & Attack Simulation Services - External Network Vulnerability Assessment - 51 to 100 external live hosts.**	Guidepoint to conduct an External Vulnerability Assessment of Client's external (Internet-facing) environment to identify vulnerabilities and weaknesses within its external environment. GuidePoint also will perform reconnaissance on Client to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of Client's environment.	$7,750.63
54151HACS	**Threat & Attack Simulation Services - External Network Vulnerability Assessment - 101 to 400 external live hosts.**	Guidepoint to conduct an External Vulnerability Assessment of Client's external (Internet-facing) environment to identify vulnerabilities and weaknesses within its external environment. GuidePoint also will perform reconnaissance on Client to uncover information that is accessible publicly that should not be. The engagement will evaluate the scope, security, and resiliency of Client's environment.	$12,675.06

PRICE LIST FOR MANUFACTURER PRODUCTS AND SUPPORT

Manufacturer	Item Number	Item Name	Item Description	GSA MAS Price	SIN
Deepwatch	DW-MDR-BASE-25-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 1-25GB daily log throughput	$143,576.83	511210
Deepwatch	DW-MDR-BASE-50-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 26-50GB daily log throughput	$192,967.25	511210
Deepwatch	DW-MDR-BASE-100-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 51-100GB daily log throughput	$280,445.74	511210
Deepwatch	DW-MDR-BASE-175-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 101-175GB daily log throughput	$374,999.70	511210
Deepwatch	DW-MDR-BASE-250-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 176-250GB daily log throughput	$490,236.37	511210
Deepwatch	DW-MDR-BASE-375-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 251-375GB daily log throughput	$642,542.67	511210
Deepwatch	DW-MDR-BASE-500-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 376-500GB daily log throughput	$799,608.06	511210
Deepwatch	DW-MDR-BASE-750-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response	$1,009,029.22	511210

			including 24x7 monitoring of up to 501-750GB daily log throughput		
Deepwatch	DW-MDR-BASE-1000-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 751-1,000GB daily log throughput	$1,224,890.28	511210
Deepwatch	DW-MDR-BASE-2500-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response including 24x7 monitoring of up to 1001-2,500GB daily log throughput	$2,426,448.36	511210
Deepwatch	DW-MDR-SETUP-A-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response One-Time Setup - 1-250GB	$47,858.94	511210
Deepwatch	DW-MDR-SETUP-B-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response One-Time Setup - 251-500GB	$95,717.88	511210
Deepwatch	DW-MDR-SETUP-C-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response One-Time Setup - 501-1,000GB	$143,576.83	511210
Deepwatch	DW-MDR-SETUP-D-FED	Managed Detection & Response (MDR)	Deepwatch Managed Detection & Response One-Time Setup - 1,001-5,000GB	$191,435.77	511210
Deepwatch	DW-VM-ESSEN-2500-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 1-2,500IP	$107,204.03	511210
Deepwatch	DW-VM-ESSEN-5000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 2,501-5,000IP	$114,861.46	511210

Deepwatch	DW-VM-ESSEN-10000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 5,001-10,000IP	$132,090.68	511210
Deepwatch	DW-VM-ESSEN-17500-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 10,001-17,500IP	$157,934.51	511210
Deepwatch	DW-VM-ESSEN-25000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 17,501-25,000IP	$180,906.80	511210
Deepwatch	DW-VM-ESSEN-50000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 25,001-50,000IP	$263,224.18	511210
Deepwatch	DW-VM-ESSEN-100000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 50,001-100,000IP	$427,858.94	511210

Deepwatch	DW-VM-ESSEN-200000-FED	Vulnerability Management (VM)	Deepwatch Vulnerability Management (VM) solutions provide vulnerability identification and management within the customer's enterprise IT environment - 100,001-200,000IP	$757,128.46	511210
Deepwatch	DW-VM-ESSEN-SETUP-A-FED	Vulnerability Management (VM)	Vulnerability Management - Essential One Time Setup - 1-5,000IP	$33,501.26	511210
Deepwatch	DW-VM-ESSEN-SETUP-B-FED	Vulnerability Management (VM)	Vulnerability Management - Essential One Time Setup - 5,001-25,000IP	$43,073.05	511210
Deepwatch	DW-VM-ESSEN-SETUP-C-FED	Vulnerability Management (VM)	Vulnerability Management - Essential One Time Setup - 25,001-200,000IP	$57,430.73	511210
Deepwatch	DW-EDR-500-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 1-500 Endpoints	$28,715.37	511210
Deepwatch	DW-EDR-1000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 501-1,000 Endpoints	$54,559.19	511210
Deepwatch	DW-EDR-1500-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy	$77,531.49	511210

			best of breed endpoint retection & response technology - 1,001-1,500 Endpoints		
Deepwatch	DW-EDR-2000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 1,501-2,000 Endpoints	$97,632.24	511210
Deepwatch	DW-EDR-3000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 2,001-3,000 Endpoints	$134,962.22	511210
Deepwatch	DW-EDR-5000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 3,001-5,000 Endpoints	$178,035.26	511210
Deepwatch	DW-EDR-7500-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint	$194,307.30	511210

			retection & response technology - 5,001-7,500 Endpoints		
Deepwatch	DW-EDR-10000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 7,501-10,000 Endpoints	$229,722.92	511210
Deepwatch	DW-EDR-15000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 10,001-15,000 Endpoints	$258,438.29	511210
Deepwatch	DW-EDR-20000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint retection & response technology - 15,001-20,000 Endpoints	$287,153.65	511210
Deepwatch	DW-EDR-25000-FED	Endpoint Detection & Response (EDR)	Deepwatch's Endpoint Detection & Response (EDR) Service offering provides customers with an experienced team to architect design, maintain, and deploy best of breed endpoint	$315,869.02	511210

			retection & response technology - 20,001-25,000 Endpoints		
Deepwatch	DW-EDR-SETUP-A-FED	Endpoint Detection & Response (EDR)	Managed Endpoint Detection & Response One-Time Setup - 1-10,000 Endpoints	$38,287.15	511210
Deepwatch	DW-EDR-SETUP-B-FED	Endpoint Detection & Response (EDR)	Managed Endpoint Detection & Response One-Time Setup - 10,000-50,000 Endpoints	$67,002.52	511210
Deepwatch	DW-EDR-SETUP-C-FED	Endpoint Detection & Response (EDR)	Managed Endpoint Detection & Response One-Time Setup - 50,001-200,000 Endpoints	$95,717.88	511210
Deepwatch	DW-FW-2-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 1-2 FW	$9,188.92	511210
Deepwatch	DW-FW-5-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 3-5 FW	$22,972.29	511210
Deepwatch	DW-FW-10-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 6-10 FW	$43,647.36	511210
Deepwatch	DW-FW-20-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 11-20 FW	$82,700.25	511210
Deepwatch	DW-FW-50-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and	$172,292.19	511210

			manage customer's firewall devices - 21-50 FW		
Deepwatch	DW-FW-100-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 51-100 FW	$298,639.80	511210
Deepwatch	DW-FW-200-FED	Firewall (FW)	Deepwatch's Managed Firewall Service provides customers with experienced engineers to monitor and manage customer's firewall devices - 101-200 FW	$459,445.84	511210
Deepwatch	DW-FW-SETUP-2-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 1-2 FW	$670.03	511210
Deepwatch	DW-FW-SETUP-5-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 3-5 FW	$1,722.92	511210
Deepwatch	DW-FW-SETUP-10-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 6-10 FW	$3,254.41	511210
Deepwatch	DW-FW-SETUP-20-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 11-20 FW	$6,221.66	511210
Deepwatch	DW-FW-SETUP-50-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 21-50 FW	$12,921.91	511210
Deepwatch	DW-FW-SETUP-100-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 51-100 FW	$22,397.98	511210
Deepwatch	DW-FW-SETUP-200-FED	Firewall (FW)	Managed Fire Wall - One Time Set Up Fee - 101-200 FW	$34,458.44	511210
Fortress Government Solutions	FGS-SCI-CLOUD-001-VA	Supply Chain Illumination Virtual Appliance	Supply Chain Illumination Virtual Appliance - Cloud License - Single Core - System includes workflows, internal/external collaboration, assessment, survey, dashboards, audit logging, role & attribute-based access, navigation, approvals, conjurable user interface, risk register, automation, event	$190,579.35	511210

			notification, supplier, product, system, and component modules. Client provides hardware or cloud infrastructure. Setup & Configuration: 6-8 week. 1 Year Term License.		
Fortress Government Solutions	FGS-SCI-CLOUD-001-MAINT	Supply Chain Illumination Virtual Appliance	Annual maintenance to support the Supply Chain Illumination Virtual Appliance - Cloud License - Single Core	$38,115.87	511210
Fortress Government Solutions	FGS-SCI-DC-001-VA	FortressGS Data Connector	1 year/1 System Data Connector and Integration Services for Supply Chain Risk Illumination. Development & Configuration: 10-12 week.	$97,733.00	511210
Fortress Government Solutions	FGS-SCI-DC-001-MAINT	FortressGS Data Connector	Technical support and software maintenance and upgrades FGS-SCI-DC-001-VA.	$19,546.60	511210
Fortress Government Solutions	FGS-SCI-CYB-VCA-MAS-001	Organization Cyber Security Vendor Control Assessment	Organization Cyber Security Vendor Control Assessment - includes full cyber assessment of vendors controls conducted by Fortress SMEs in collaboration with vendor. Turn Around time: 5-7 days	$5,668.51	511210
Fortress Government Solutions	FGS-SCI-CYB-SRCH-1K-001	Organization Cyber Security Illumination Data Cartridge	Organization Cyber Security Illumination Data Cartridge - Includes automated risk illumination for a given organization, revealing application security, security protocol health, domain configuration, geolocation, and patching cadence. Turn Around time: 1-2 days	$56.69	511210

Fortress Government Solutions	FGS-SCI-PRD-OSINT-25-001	OSINT Product Cyber Risk Illumination - Product Reports	OSINT Product Cyber Risk Illumination - Product Reports - Risk illumination is provided for product vulnerability history, vulnerability notice procedures, patching cadence, and 65 product security controls are validated based on publicly-available information such as product guides and web searches. Turn Around time: 5-7 days	$4,251.39	511210
Fortress Government Solutions	FGS-SCI-PRD-SBOM-M-05-001	Vulnerability and Foreign Influence Analysis	Vulnerability and foreign influence analysis of manufacturer- provided software bill of materials. Risk illumination is provided for product vulnerability history, vulnerability notice procedures and patching cadence are validated based on publicly-available information such as product guides and web searches. Foreign influence is identified on all identified fourth parties. Turn Around time: 2-4 weeks	$11,337.03	511210
Fortress Government Solutions	FGS-SCI-PRD-HBOM-M-05-001	Vulnerability and Foreign Influence Analysis	Vulnerability and foreign influence analysis of manufacturer- provided hardware bill of materials. Risk illumination is provided for product vulnerability history, vulnerability notice procedures and patching cadence are validated based on publicly-available information such as product guides and web searches. Foreign influence is identified	$11,337.03	511210

			on all identified fourth parties. Turn Around time: 2-4 weeks		
Fortress Government Solutions	FGS-SCI-PRD-SHBOM-M-05-001	Vulnerability and Foreign Influence Analysis	Vulnerability and foreign influence analysis of manufacturer- provided software and hardware bill of materials. Risk illumination is provided for product vulnerability history, vulnerability notice procedures and patching cadence are validated based on publicly- available information such as product guides and web searches. Foreign influence is identified on all identified fourth parties. Turn Around time: 2-4 weeks	$17,005.54	511210
Fortress Government Solutions	FGS-FIA-PROD-100-001	Monitoring	Monitoring - Software Supply Chain - File Integrity & Authenticity (FIA) Product Subscription Cartridge - 100 Products - Annual subscription to a File Integrity & Authenticity Assurance process, validating the authenticity and integrity of all patches and updates for a given product. Authenticity checks include checking the supplier for known breaches, appropriate encryption delivery, updated security certificate and DNS checks. Integrity checks include	$850.28	511210

			reviewing code signage, malware analysis and in some cases sandbox and firmware analysis. Turn Around time: 1-2 days		
Fortress Government Solutions	FGS-SCI-PRD-OSINT-MON-25-001	Monitoring	Monitoring - Product Cyber Risk Illumination Cartridge - Annual subscription for products to monitor supply chain risk in products from software and firmware vulnerabilities to threat alerts to patching cadence to product obsolescence. Turn Around time: 5-7 days	$1,417.13	511210
Fortress Government Solutions	FGS-SCI-CYB-MON-100-001	Monitoring	Organization Cyber Security Illumination Monitoring Cartridge - Includes annual subscription for automated risk illumination for a given organization, revealing application security, security protocol health, domain configuration, internet protocol reputation, geolocation and patching cadence. Turn Around time: 5-7 days	$226.74	511210
Secure Code Warrior	SCW-LEARNING-PLATFORM-ANNUAL	SCW Learning Platform	Per End User annual subscription to Secure Code Warrior Learning Platform; 25 End User minimum.	$488.16	511210

COMMERCIAL SUPPLIER AGREEMENTS

Deepwatch

Master Subscription Agreement
version 2022 05 02

THIS MASTER SUBSCRIPTION AGREEMENT ("MSA") IS EFFECTIVE AS OF THE DATE SET FORTH IN THE ORDER FORM ("EFFECTIVE DATE") AND GOVERNS THE SERVICES (AS DEFINED BELOW) TO BE PROVIDED BY DEEPWATCH FEDERAL, INC. (HEREINAFTER REFERRED TO AS "Deepwatch"), ITS AFFILIATES, AND/OR ITS OR THEIR SUPPLIERS, RESELLERS, DISTRIBUTORS, SERVICE PROVIDERS, AND/OR LICENSORS (COLLECTIVELY REFERRED TO AS "SUPPLIERS") TO THE ORDERING ACTIVITY UNDER GSA SCHEDULE CONTRACTS IDENTIFIED IN THE ORDER FORM ("CUSTOMER"), PURSUANT TO AN ORDER FORM (AS DEFINED BELOW). BY EXECUTING AN ORDER FORM, CUSTOMER IS ACCEPTING AND AGREEING TO THIS MSA AND THE TERMS OF SUCH ORDER FORM WHICH, UPON EXECUTION BY CUSTOMER, BECOMES PART OF AND SUBJECT TO THIS MSA. EACH ORDER FORM EXECUTED BY CUSTOMER SHALL BE EFFECTIVE AS OF THE EFFECTIVE DATE SPECIFIED THEREIN OR, IF NO EFFECTIVE DATE IS SPECIFIED, THE DATE CUSTOMER EXECUTES THE ORDER FORM. DEEPWATCH AND CUSTOMER MAY BE REFERRED TO INDIVIDUALLY AS A "PARTY" AND, COLLECTIVELY, AS THE "PARTIES".

1. Definitions

"Affiliate" of a Party means any other entity that, directly or indirectly, controls, is controlled by, or is under common control with, such Party. "Control", for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity or the power to direct or cause the direction of the management and policies of such entity.

"Customer" may also include any Customer Affiliate: (i) receiving the benefit of the Services through Customer's purchase of the Services, or (ii) whose data is included, accessed, or received by Deepwatch in connection with the performance and/or provision of the Services for Customer. With respect to such Customer Affiliate(s), Customer hereby represents and warrants that: (a) Customer has obtained the necessary consent from each Customer Affiliate for Deepwatch to access such Customer Affiliate's networks and data in connection with providing the Services; and (b) each Customer Affiliate agrees to, and is hereby legally bound by, the terms of this MSA. The parties acknowledge and agree that Customer Affiliates are not intended to be third party beneficiaries to this MSA unless contracting directly under an applicable Order Form pursuant to this MSA. Customer shall be fully liable for any breach of the terms of this MSA by any Customer Affiliate receiving, using, or having access to the Services.

"Customer Data" means any and all data, information and material either transmitted or uploaded by Customer into applicable Third Party Software for use in performance of the Services. Except as set forth in Section 2.3(e), Customer Data shall not include or contain any Personal Data.

"Deficiency" means a material failure to meet a SLA (as described below) or a material error in a Deliverable.

"Deliverable(s)" means any reports or custom dashboards created for Customer by Deepwatch.

"Documentation" means Deepwatch's electronic and/or hard copy Service Descriptions, user guides, help and training materials, and other documentation for the Services, which may be updated, amended, or replaced by Deepwatch from time to time in its sole discretion.

"EULA" means a third party vendor's end user license agreement, subscription agreement, services agreement, or similar
document for use of or access to any Third Party Software.

"Law" means any local, state, federal, administrative, and/or foreign laws, statutes, treaties, regulations, and/or court or regulatory agency orders applicable to a Party.

"Log File" means a file that records security events that occur in software used by Customer. In the case of any Customer Log Files provided to or accessed or processed by Deepwatch, Customer shall ensure that Log Files do not contain any Personal Data. Notwithstanding the foregoing sentence, for purposes of this MSA, it is permissible for Customer's Log Files to contain IP and MAC addresses, computer hostnames, a User's name and location, email addresses, badge information, and employee ID numbers.

"Order Form" means any ordering document, proposal, and all attachments thereto, for the purchase of the Services set forth

therein, that is executed by Deepwatch or a Reseller of the Deepwatch Services and Customer. Each executed Order Form is incorporated herein and subject to the terms of this MSA.

"Personal Data" means any non-public information and/or data that can be used, alone or in combination with other data, to identify any individual person. Personal Data includes, without limitation, a person's home address, date of birth, social security number, home or personal telephone numbers, credit card information, driver's license number or unique number contained in any other government-issued identification document, bank account numbers, mother's maiden name and any other information used to authenticate identity, biometric records, Personal Health Information (as that term is defined and/or used in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health Act) or any other medical information, education information, any passport and/or visa number, passwords, financial information, and/or any employment information. In light of the sensitive nature of Personal Data, Customer shall not send, provide, and/or make accessible to Deepwatch any Personal Data unless such Personal Data is required and needed for a specific project assigned by Customer to Deepwatch and agreed to in writing by Deepwatch. In any such situation, Customer shall only send, provide, or make accessible to Deepwatch the specific Personal Data which Deepwatch needs to access and/or use

in order to provide the specific services requested by Customer pursuant to this MSA, an Order Form or proposal agreed to in writing between Customer and Deepwatch.

“Reseller” means any reseller and/or distributor of the Services who completes Order Form fulfillment for the Deepwatch Services. Such Reseller shall be responsible for any payments related to Deepwatch’s Services pursuant to the Order Form and Resellers invoice or purchase order for such Services.

“Services” means Deepwatch’s proprietary managed security subscription services and associated modules, components, and updates thereto and any related services provided by Deepwatch under an Order Form.

“Services Description” means a detailed outline of the managed services that Deepwatch or a reseller or distributor of the Deepwatch Services will provide per the Order Form and can also be found on the Deepwatch web page as set forth at https://legal.Deepwatch.com.

“Subscription Term” means the period of time Services are contracted for under an Order Form as may be renewed or modified
by a change order.

“Third Party Software” means any third party (e.g., Splunk, ServiceNow) software (including components subject to the terms and conditions of “open source” software licenses) and/or other third party copyrighted and/or proprietary products, documentation, materials, and services (including any features, functionality, and updates), extensions (including any separate downloadable suite, add-on, command, function, or application, including any module, which extends a software program) as well as any modifications to any such software and any derivatives of any of them provided with or required in performance of the Services, of which such software (a) is or may be directly licensed or subscribed to by Customer and provided or made accessible to Deepwatch by Customer for Deepwatch to perform managed Services as set forth in the applicable Order Form (“Customer Third Party Software”), or (b) is directly licensed or subscribed to by Deepwatch and may be made accessible by Deepwatch to Customer, or may be internally used by Deepwatch in performance of the Services, but in neither case will Customer be the direct licensee (“Deepwatch Third Party Software”). Customer Third Party Software and Deepwatch Third Party Software are collectively referred to as the Third Party Software.

2. Services

2.1 Provision of the Services.

(a) Deepwatch will make the Services available pursuant to the terms of this MSA and each Order Form during the applicable Subscription Term to (i) Customer; and (ii) each individual employee, consultant, contractor, and agent who is authorized by Customer to access and/or use the Services during the Subscription Term (each, a “User”) and subject to the usage restrictions, limits, and/or conditions set forth in this MSA as well as the applicable Services Description and/or Order Form. If the

Services will be made available to any Customer Affiliate pursuant to this MSA, then the term "Customer" shall also include any such Customer Affiliate. Customer understands and acknowledges that Deepwatch may use Third Party Software

in its performance and provision of the Services including components subject to the terms and conditions of open source software licenses. Deepwatch Third Party Software incorporated in its Services does not require an additional license or sublicense to be secured by Customer. Notwithstanding the foregoing, Customer acknowledges that it is responsible for securing licenses and/or subscriptions for any Customer Third Party Software required for Deepwatch's use during the Subscription Term in order to provide Services to Customer.

(b) Customer understands and agrees that Customer data may be hosted on public cloud service providers (by way of example, ticketing, threat intelligence, SOAR and remote access). Any data stored by Deepwatch on a public cloud service provider will be protected by industry standard security best practices in accordance with Deepwatch's regulatory obligations. The Services made available under this MSA do not include any implementation, professional, advisory, or technical services which Customer may purchase separately from Deepwatch or a Reseller pursuant to the terms set forth in a Statement of Work or Services Description describing such services (the "Professional Services"). Customer may incur additional Fees for exceeding any defined volume or user limits applicable to any of the Services as documented in an Order Form.

(c) Background Screening. Deepwatch shall ensure that prior to assignment all employees, agents and subcontractors who will have access to Customer Data, have favorably completed background screening requirements which include the following at a minimum:

- SSN Validation
- Employment Verification (Last 7 years)
- Education Verifications
- Address History in accordance to applicable State Law (Last 7 years)
- National Criminal Records in accordance to applicable State Law (Last 7 years)
- County Criminal Records in accordance to applicable State Law (Last 7 years for all counties of residence)
- Federal and State Criminal Search
- Sex Offender List
- FACIS
- Terrorists Watch List
- OFAC Sanctions List
- Denied Persons List
- Unverified List
- Drug Screen

2.2 Updates; Future Features and Functionality.

Deepwatch will make available to Customer and Users all updates and enhancements to the Services that Deepwatch generally makes commercially available to its customers. Customer agrees that the development, release, and timing of any features or functionality for the Services remains at Deepwatch's sole discretion and Customer's purchase of the Services is not contingent or dependent on the delivery of any future functionality, feature, or other services or products regardless of any communications about Deepwatch's plans, including any information on Deepwatch's website or in any presentation, proposal, press release, or public statement. From time to time, Deepwatch may provide Customer with a maintenance update to any of the Services. All warranties, indemnification obligations, and duties of Deepwatch are conditioned upon Customer's acceptance, and if applicable, reasonably prompt installation of all maintenance updates supplied or made accessible by Deepwatch or its Supplier as directed.

2.3 Controls, Policies, and Procedures.

(a) Security Certifications. Deepwatch maintains internal controls, policies, and procedures at least as effective as those described in Deepwatch's most recent SOC 2 Type 2 report ("SOC Report"). Additionally, Deepwatch meets or exceeds the Payment Card Industry ("PCI") Security Standards Council ("SSC") requirements for Level 1 Service Providers, as attested to in Deepwatch's most recent PCI Data Security Standard Attestation of Compliance ("AoC") for Onsite Assessments – Service Providers report ("PCI Report") and has obtained TRUSTe Enterprise Certification.

(b) Cardholder Data. While Deepwatch is a PCI Compliant Service Provider, it is incumbent upon Customer to ensure that it does not share any cardholder data ("CHD") with any Deepwatch Services and/or upload any CHD into the Deepwatch security platform. In the unlikely event Customer inadvertently discloses CHD to Deepwatch or upload any CHD into the Deepwatch security platform, Customer is required to notify Deepwatch in writing, as soon as practicable, and assist Deepwatch in identifying, anonymizing, and/or removing the disclosed and/or uploaded CHD.

(c) Security Reports. Upon Customer's written request, (and execution of a mutual non-disclosure agreement if such information is required prior to execution of this MSA), Deepwatch will provide Customer with the most recent copy of either the SOC Report, PCI Report, and/or TRUSTe Certification. These reports, and any analyses, reports, summaries, and/or information related to or derived from such reports, are considered Deepwatch's Confidential Information (as defined below).

(d) Security Questionnaires. Deepwatch defers all responses to Customer cybersecurity questionnaires until Customer has reviewed the above reports and completed Customer's questionnaire utilizing the information contained within the reports.

(e) Customer Personal Data. Except for information contained in any Log Files processed by Deepwatch, Customer shall neither disclose to Deepwatch nor upload into or process in the Deepwatch security platform or make accessible to any Deepwatch service, personnel, or contractor any Personal

Data of any nature and/or any other non-public personally identifiable information other than information contained in Log Files that could be legally considered private or sensitive. Notwithstanding the above, in the event that Customer uploads Personal Data and/or any other non-public personally identifiable information that could be legally considered private or sensitive or makes any Personal Data accessible in any Deepwatch service offering in violation of this MSA, Customer shall remove such Personal Data immediately or, at its reasonable discretion, Deepwatch may purge such data from the applicable Third Party Software and system and all Deepwatch services.

(f) Collection of Customer Data. Customer is responsible for all activities that occur in the Customer account and for each User's compliance with all terms and conditions of this MSA. Customer is responsible for the collection, legal protection, and use of all Customer data that is loaded, stored, accessible, or used in connection with Customer's use of any Deepwatch services.

(g) Privacy Compliance. Each Party shall comply with all local, state, federal and foreign laws, treaties, regulations, and conventions to the extent applicable to such party in connection with its provision, access to, and/or use of the Services, including, without limitation, the General Data Protection Regulation ("GDPR"), CAN-SPAM Act of 2003 (U.S.A.), the Personal Information Protection and Electronic Documents Act ("PIPEDA") (Canada), California Consumer Privacy Act ("CCPA"), and all other applicable state privacy laws, the EU Data Protection Directive, and all other laws and regulations applicable to Customer Data related to privacy, publicity, data protection, electronic communications, and anti-spamming laws

2.4 Service Level Agreement.

Deepwatch provides its customers with Service Level Agreements ("SLA") including the system uptime availability commitment for the Services as described in the SLA as set forth in each applicable Order Form attached hereto as Exhibit A, as may be non-materially amended from time to time by Deepwatch in its sole discretion. Customer's sole and exclusive remedy, and Deepwatch's sole and exclusive liability, for failure to satisfy the applicable availability commitment is set forth in the SLA.

3. Fees

3.1 Invoice and Payment.

All fees for the Services ordered by Customer (collectively, the "Fees" or "Subscription Fees") shall be pursuant to an executed Order Form and all Fees are quoted and payable in United States dollars as agreed upon between Customer and the Reseller. All Fees are based on the Services ordered by Customer in any Order Form and not actual usage. Except as otherwise set forth in this MSA, quantities ordered cannot be decreased during the relevant Subscription Term.

3.2 Reserved

3.3 Billing Disputes.

Any dispute involving invoiced Fees (a "Billing Dispute") must be in writing and submitted in good faith to the Reseller within thirty (30) days of the invoice date and include a reasonably detailed statement describing the nature and amount of the disputed Fees as well as the reasonable and good faith basis for why a credit or refund is being requested (a "Billing Dispute Notice"). Customer shall cooperate with the Reseller to promptly address and attempt to resolve any Billing Dispute submitted by Customer. Notwithstanding any dispute of invoiced Fees commenced in accordance with this Section 3.3, Customer shall remain obligated to pay all undisputed Fees within thirty (30) days of the invoice receipt date or as otherwise applicable. Notwithstanding anything to the contrary in this Agreement, non-payment by the Customer of a disputed invoice pursuant to this Section 3.3 will not be considered a default by the Customer and will not be considered grounds for termination of this Agreement.

4. Proprietary Rights

4.1 Ownership.

Deepwatch and/or its Suppliers own all worldwide right, title, and interest in and to the Services (including the Documentation), and Third Party Software, including all worldwide patent rights (including patent applications and disclosures); copyright rights (including copyrights, copyright registrations, and copyrights with respect to computer software, software design, software code, software architecture, firmware, programming tools, graphic user interfaces, documentation, reports (except reports specifically prepared by Deepwatch for Customer), dashboards, business rules, use cases, screens, alerts, notifications, drawings, specifications and databases); moral rights; trade secrets and other rights with respect to confidential or proprietary information; know-how; other rights with respect to inventions, discoveries, ideas, improvements, techniques, formulae, algorithms, processes, schematics, testing procedures, technical information and other technology; and any other intellectual and industrial property rights, whether or not subject to registration or protection; and all rights under any license or other arrangement with respect to any of the foregoing. Deepwatch does not grant Customer any intellectual property rights in or to the Services, Documentation, or any Third Party Software, and all right, title, and interest in and to all copies of the Services, Documentation, and Third Party Software will remain with Deepwatch and/or its Suppliers. Deepwatch owns and shall continue to own all right, title, and interest in and to the Services and Documentation (except for any Third Party Software incorporated therein, which shall remain the sole property of the Supplier, as applicable). Deepwatch and/or its Suppliers may modify and/or improve the Services, Third Party Software, and/or any Documentation at any time and Deepwatch's and its Suppliers' ownership rights (including all intellectual property rights) will include all enhancements, modifications, adaptations, and/or derivative works therein and thereto (whether made by Deepwatch, any third party, or jointly). Notwithstanding the foregoing, Customer shall have the right for continued use after termination or expiration of this MSA of any Deliverables provided during the Subscription Term, provided however, any Deliverables provided through or by Third Party Software shall be licensed per the applicable EULA.

4.2 Grant of Rights.

This is an agreement for use of Deepwatch services and not an agreement for the sale or license of any software or Third Party Software or the sale or license of any Deepwatch Third Party Software unless otherwise specified in an Order Form. Deepwatch hereby grants Customer a limited, worldwide (subject to export Laws), non-exclusive, non-transferable, revocable right to use the Services (including the Documentation), solely for the internal business purposes of Customer and solely during the Subscription Term, subject to the terms and conditions of this MSA and scope of use described in the relevant Order Form. No rights are granted to Customer hereunder other than as expressly set forth herein and Deepwatch, and/or its Supplier if applicable, reserves all rights not specifically granted under this MSA.

4.3 Customer Obligations; Grant Restrictions.

(a) Customer Obligations. Customer shall not (or allow any person, Affiliate, and/or entity to): (i) modify, copy, or create any derivative works based on the Services; (ii) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, timeshare, offer in a service bureau, or otherwise make the Services available to any third party, other than to Users as permitted herein; (iii) reverse engineer, disassemble, or decompile any portion of the Services, including any software utilized by Deepwatch in the provision of the Services, except to the extent required by Law; (iv) access the Services if it (or any Affiliate) is a direct competitor of Deepwatch or in order to build any competitive or commercially available product or service or for purposes of monitoring the availability, performance, or functionality of the Services, or for any other benchmarking or competitive purposes; (v) copy any features, functions, integrations, interfaces, or graphics of the Services; (vi) use the Services in violation of any Laws or outside the scope of the rights granted in Section 4.2; (vii) in connection with the Services, send or store any material that (a) infringes or misappropriates any intellectual property right of Deepwatch, any Supplier, or any other third party, or (b) is obscene, threatening, or otherwise unlawful or tortious or violates any Laws or other party's rights, including any privacy, publicity, import and export control, data protection, electronic communications, or anti-spamming Laws or rights; (viii) send or store any viruses, worms, time bombs, Trojan horses, and other harmful or malicious code, files, scripts, agents, or programs ("Malicious Code") in connection with the Services; (ix) interfere with or disrupt performance of the Services or the data contained therein; or (x) attempt to gain access to the Services or its related systems or networks in a manner not set forth in the Documentation related to such Services. With respect to Deepwatch's Third Party Software and the Deepwatch security platform, Customer shall also not (1) cause or permit the disclosure, copying, renting, licensing, sublicensing, leasing, dissemination or other distribution of any such software and/or the Deepwatch security platform by any means or in any form, (2) use any such software and/or the Deepwatch security platform to conduct a service bureau or similar business for the benefit of any third party, or (3) modify, enhance, supplement, create derivative work from, adapt, translate, reverse engineer, decompile, disassemble or otherwise reduce the software and/or the Deepwatch security platform to human readable form. Customer shall have sole responsibility for the collection, accuracy, quality, integrity, legality, reliability, appropriateness, legal protection, and use rights of all Customer Data (as defined below). Customer will cause its Affiliates (and

each Affiliate's Users) who have access to and/or use the Services to comply with the provisions of this MSA and shall be responsible and liable for the acts, errors, negligence, and/or omissions of all Users and each Affiliate's Users relating to this MSA and/or the use of any Services.

(b) Grant Restrictions. Customer acknowledges that Deepwatch's performance and delivery of the Services are contingent upon: (i) Customer providing safe and hazard-free access to its personnel, facilities, equipment, network, and information, and (ii) Customer's timely decision-making and provision of timely, accurate and complete information and reasonable assistance, including, granting of approvals or permissions, as subsections (i) and (ii) are deemed reasonably necessary and reasonably requested for Deepwatch to perform, provide, and/or implement the Services. Customer will promptly obtain and provide to Deepwatch any required licenses, approvals, and/or consents necessary for Deepwatch's performance or provision of the Services. Deepwatch will be excused from its failure to perform its obligations under this MSA to the extent such failure is caused by Customer's delay in performing or failure to perform its responsibilities under this MSA and/or any Services Description as provided in each applicable Order Form.

4.4 Ownership and Use of Customer Data; Data Processing.

Customer owns all right, title and interest in and to all Customer Data. Subject to the terms of this MSA, Customer grants Deepwatch and its Affiliates a worldwide, limited, royalty-free, non-exclusive, non-transferable (except as set forth in Section 10.6) license (where applicable) and right to (a) access, use, copy, transmit, and display Customer Data in order to provide the Services and any Professional Services to Customer (including the ability to address service and/or technical problems and/or maintain and monitor usage of the Services); and (b) de-identify and aggregate Customer Data with data of other customers or third parties such that it does not reveal the identity of any individual or include personally identifiable information ("Aggregated Data") to perform analytics and reporting for system metrics, benchmarking, product development, and marketing for industry, financial, and other business purposes; and (c) enforce the rights of the Parties under this MSA, as may be applicable. Customer reserves all rights in Customer Data not expressly granted to Deepwatch.

4.5 All Customer owned and/or provided products embedded in, supported by, or essential to use of Active Maintenance and/or access to the Services must have active maintenance agreements. Customer is responsible for all maintenance, support, and licensing agreements with third party vendors for all non-Deepwatch provided in-scope devices during the Subscription Term. Customer shall also be responsible for the application, operation, maintenance, and support of its systems including all hardware and software and all components thereof including, without limitation, the implementation of appropriate procedures, training, and safeguards and performing routine backup and for keeping backup information in a safe and

separate location. Deepwatch shall not be required to support altered, damaged, or modified software, or software that is running a non-vendor-supported version (including any firmware).

4.6 Use of Customer Input.

Customer grants Deepwatch a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into Deepwatch's products and services any suggestion, enhancement request, recommendation, correction, or any other feedback provided by Customer or any User relating to the Services

5. Confidentiality

5.1 Confidential Information; Exceptions.

"Confidential Information" means all non-public information disclosed by a Party ("Disclosing Party") to the other Party ("Receiving Party"), whether verbally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and/or the circumstances of disclosure. Customer Confidential Information includes Customer Data; Deepwatch Confidential Information includes the Services (including all Documentation); and Confidential Information of each Party includes business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed or made accessible by such Party. Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party; (iii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party; (iii) is received from a third party without breach of any obligation owed to the Disclosing Party; or (iv) was independently developed by the Receiving Party without access to or reliance on the Disclosing Party's information.

5.2 Protection.

The Receiving Party will use the same degree of care that it uses to protect the confidentiality of its own Confidential Information of like kind (but not less than reasonable care) to (i) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this MSA or any Order Form; and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclosing Party to those of its and any of its Affiliate's employees, officers, advisors, contractors, and third parties (collectively, "Representatives'') who need access for purposes consistent with this MSA and who have signed confidentiality agreements with the Receiving Party containing protections, or have ethical duties to the Receiving Party, not materially less protective of the Disclosing Party's Confidential Information than those set forth in this MSA. Each Party shall be and remain fully liable and responsible for any of its Representative's unauthorized disclosure, access to, and/or use of the other Party's Confidential Information. Each Party may confidentially disclose the terms of this MSA (including any Order Form) to any actual or potential financing source or acquirer. Notwithstanding the foregoing, Deepwatch may disclose the terms of this MSA and any applicable Order Form to a subcontractor to the extent necessary to perform or satisfy Deepwatch's obligations to Customer under this MSA and/or any Order Form, under terms of confidentiality materially as protective as set forth in

this MSA. Deepwatch shall not be liable nor responsible for any breach of this Section 5 ("Confidentiality") resulting from (i) Customer's violation of Section 2.3(e) above and/or to the extent Customer uploads into or processes in the Deepwatch security platform or makes accessible to any Deepwatch service, personnel, or contractor any Personal Data; or (ii) any hack or intrusion by a third party (except any Deepwatch third party subcontractor) into Customer's network or systems unless the hack or intrusion was through endpoints or devices monitored by Deepwatch and was caused directly by Deepwatch's gross negligence or willful misconduct.

5.3 Misuse of Confidential Information.

Customer acknowledges and agrees that the Services contain proprietary information and trade secrets of Deepwatch and its Suppliers. Customer will not use any Confidential Information or know how that it gains through use or study of the Services to facilitate Customer's or any third party's development of any services or products that would compete with the Services provided by Deepwatch. Subject to Deepwatch's confidentiality obligations, Deepwatch reserves the right to develop and

market any technology, products, and/or services or pursue business opportunities that compete with and/or are similar to those of Customer.

5.4 Compelled Disclosure; Retention.

The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by Law to do so, provided that, to the extent legally permissible, the Receiving Party gives the Disclosing Party prior written notice of the compelled disclosure and, at the Disclosing Party's cost, reasonable assistance if the Disclosing Party wishes to contest the disclosure or limit the extent of the disclosure through a protective order or other legal measure. If the Receiving Party is compelled by Law to disclose the Disclosing Party's Confidential Information as part of a legal proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to that Confidential Information. Notwithstanding anything to the contrary contained herein, (i) the Receiving Party may retain such copies of the Disclosing Party's Confidential Information as are reasonably necessary: (1) to comply with any Laws or regulations applicable to Receiving Party or to comply with the Receiving Party's document retention policies; and/or (2) for the purposes of defending or maintaining litigation; and (ii) in no event shall this MSA require the alteration, modification, deletion, or destruction of back-up tapes, archived data storage, or other media made in the ordinary course of business provided that the terms and conditions of this MSA shall apply to the Receiving Party's retention of any of Disclosing Party's Confidential Information and survive the termination or expiration of this MSA for any reason. Deepwatch recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

5.5 General Data Protection Regulation.

To the extent applicable to Deepwatch and taking into account Customer's obligations under Section 2.3(e) above, Deepwatch agrees to comply with General Data Protection Regulation 2016/679 per the internal guidelines located at https://legal.Deepwatch.com/gdpr.

6. Representations, Warranties, Exclusive Remedies & Disclaimers

6.1 Warranties.

Each Party represents and warrants that it has the authority to enter into this MSA and, in connection with its performance of this MSA, shall comply with all Laws.

6.2 Deepwatch Warranties.

Deepwatch also represents and warrants during the applicable Subscription Term: (a) the Services will perform materially in accordance with the applicable Services description related to such Services; and (b) it will use commercially reasonable efforts to prevent the introduction by Deepwatch of Malicious Code into Customer's systems (excluding any Malicious Code introduced by Customer or any of its Users to the Services). All Deepwatch warranties are solely for the benefit of Customer and for no other entity or third party. Deepwatch shall not be responsible for any breach of any the foregoing warranties resulting from Customer's or its User's abuse or misuse of any Service, breach of this MSA or applicable Order Form, or failure to use any Service as described in this MSA, including failure to use any Service in accordance with the applicable Services description and operational requirements.

6.3 Customer Warranties.

Customer also represents and warrants that all information pertaining to scanning Services such as Customer-provided IP addresses and devices functioning at those IP addresses are owned or controlled by Customer and Customer is legally entitled to authorize that scanning Services be performed upon such IP addresses. To the extent Customer is a Covered Entity as defined under the HIPAA, as amended, Customer shall (i) implement the administrative, physical, and technical safeguards required by 45 C.F.R. 164.314, and (ii) implement appropriate safeguards in accordance with §13401 of HITECH and any regulations or guidance promulgated thereunder to prevent disclosure and/or transmission to Deepwatch of (1) any data not specifically required to be provided as set forth in an Order Form, and/or (2) any other data unless Deepwatch otherwise agrees in writing to accept, consistent with the standards for privacy and security of individually identifiable health information as set forth at 45 C.F.R. Parts 160 and 164, or to fully encrypt the data to meet requirements in 45 C.F.R. Part 164.312.

6.4 Ultrahazardous Activities.

Customer acknowledges and agrees that the Services and any Third Party Software are not designed, manufactured, or intended for use in any environment in which the failure of the Services and/or Third

Party Software could lead to death, personal injury, and/or physical or environmental damage, which uses and environments may include, but are not limited to, the design or operation of nuclear facilities, aircraft navigation, or communication systems, air traffic control, direct life support machines, or weapons systems or the on-line control of equipment in any hazardous environment requiring fail-safe performance. Customer represents and warrants that Customer will not install or use the Services and/or any Third Party Software for any such purposes.

6.5 Exclusive Remedies.

As Customer's sole and exclusive remedy and Deepwatch's sole and exclusive liability for breach of the warranties set forth in Section 6.2(a) above, (i) Deepwatch shall correct the material deficiency of the affected Service at no additional charge to Customer; and (ii) if Deepwatch is unable to correct the material deficiency of the affected Service after its good faith efforts, Deepwatch or the Reseller shall, in its discretion, either refund to Customer a pro-rata portion of the amounts of any prepaid Fees attributable to the materially deficient Service from the date Deepwatch received such written notice from Customer or extend the Subscription Term then in effect for a period of time equal to the time period that the materially deficient Services were provided by Deepwatch. To receive any warranty remedies, Customer must promptly report any Deficiency in writing to Deepwatch, but no later than thirty (30) days after the Deficiency has first occurred.

6.6 DISCLAIMERS.

EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 6, NEITHER PARTY MAKES ANY WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE (INCLUDING NON- INFRINGEMENT), AND ANY IMPLIED WARRANTY ARISING FROM STATUTE, COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE, TO THE MAXIMUM EXTENT PERMITTED BY LAW. EXCEPT FOR THE ACT, ERROR, NEGLIGENCE, OR OMISSION OF A USER, EACH PARTY DISCLAIMS ALL LIABILITY AND INDEMNIFICATION OBLIGATIONS FOR ANY HARM OR DAMAGES CAUSED BY ANY THIRD PARTY. DEEPWATCH DOES NOT WARRANT THAT THE SERVICES WILL BE ERROR FREE OR UNINTERRUPTED AND DEEPWATCH SHALL NOT BE RESPONSIBLE FOR ANY LIMITATIONS, DISRUPTIONS, DELAYS, AND/OR OTHER PROBLEMS INHERENT IN THE USE OF THE INTERNET AND/OR ANY ELECTRONIC COMMUNICATION. Notwithstanding anything herein to the contrary, Deepwatch and its Suppliers make no warranties with respect to any portion of any deliverable or any third party software, deliverable, products, and/or services.

7. Indemnifications

7.1 Indemnification by Deepwatch.

Deepwatch shall, at its expense, have the right to intervene to defend, indemnify, and hold Customer, its officers, directors, employees, and contractors and Affiliates (collectively, "Customer Indemnitees)

harmless from and against any and all third party claims, demands, suits, or proceedings ("Claims") against Customer, and/or any Customer Indemnitee, alleging that the use of the Services (excluding any Customer Third Party Software) in accordance with this MSA and all Order Forms infringes any U.S. patent issued as of the Effective Date, copyright, or trademark of a third party, and shall pay all costs and damages finally awarded against Customer by a court of competent jurisdiction as a result of any such Claim; provided, however, that Customer: (i) promptly gives written notice of the Claim to Deepwatch; (ii) gives Deepwatch sole control of the defense and settlement of the Claim (provided that Deepwatch may not settle any Claim or enter into any stipulated order or judgment that purports to bind Customer unless it unconditionally releases Customer of all liability); and (iii) provides to Deepwatch, at Deepwatch's cost, all reasonable assistance requested by Deepwatch. Deepwatch shall not be required to indemnify Customer in the event of: (1) modification of any Services in any manner by Customer, its employee, agent, contractor, or any User or as a result of any prohibited activity as set forth herein; (2) use of the Services in violation of this MSA, in any unauthorized manner, or in any manner inconsistent with the Documentation; (3) use of any Services in combination with any other product, service, and/or software not provided by Deepwatch or approved, and/or specified by Deepwatch in writing prior to such combined use; or (4) any infringement or misappropriation of any intellectual property right arising from or related to the access to and/or use of any Customer Third Party Software contained within any of the Services and/or Documentation. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516 or Deepwatch's right to co-defend any IP Infringement Claims. If (a) Customer is enjoined from using any Services for any reason; or (b) any of the Services becomes, or Deepwatch believes the Services are likely to become, the subject of an infringement Claim, then Deepwatch shall have the right, in its sole discretion, to (y) obtain for Customer the right to continue use of the affected Services; or (z) replace or modify the affected Services so that they are no longer infringing. If neither of the foregoing options is reasonably available to or commercially feasible for Deepwatch, then Deepwatch and/or the Reseller, in its sole discretion, may terminate the affected Services and Deepwatch's as well as the Reseller's sole liability shall be to provide Customer a pro-rata refund of any prepaid Fees attributable to the affected Services that were to be provided after the effective date of termination. THIS SECTION 7.1 SETS FORTH DEEPWATCH'S AS WELL AS ANY SUPPLIER'S SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT BY DEEPWATCH OR ANY OF ITS AFFILIATES.

7.2 Reserved.

8. Damages Exclusions; Limitation of Liability; Mitigation of Damages

8.1 Exclusion of Consequential and Related Damages; Limitation of Liability.

TO THE MAXIMUM EXTENT PERMITTED BY LAW AND EXCEPT WITH RESPECT TO CUSTOMER'S PAYMENT OBLIGATIONS UNDER THIS MSA AND ALL ORDER FORMS, IN NO EVENT SHALL (I) EITHER PARTY OR ITS SUPPLIERS, AFFILIATES, DIRECTORS, OFFICERS, EMPLOYEES, AGENTS, AND/OR CONTRACTORS HAVE ANY

LIABILITY TO THE OTHER PARTY OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, COVER, RELIANCE, PUNITIVE, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY KIND, HOWEVER CAUSED, AND/OR FOR ANY LOSS OF ANY BUSINESS, REVENUE, ANTICIPATED SAVINGS AND/OR PROFITS, USE, AND/OR LOSS OR CORRUPTION OF ANY DATA AND/OR COST OF DATA RECONSTRUCTION OR PROCUREMENT OF SUBSTITUTE OR REPLACEMENT GOODS, SERVICES, INVENTORY, OR EQUIPMENT, WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR UNDER ANY OTHER THEORY OF LIABILITY, ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THIS MSA, ANY ORDER FORM, AND/OR THE PROVISION OF ANY SERVICES, EVEN IF SUCH PARTY HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF ANY SUCH LOSS AND/OR DAMAGE; AND (II) EITHER PARTY'S ENTIRE AND MAXIMUM LIABILITY ARISING OUT OF OR RELATED TO THIS MSA AND ALL ORDER FORMS, WHETHER IN CONTRACT, TORT, STRICT LIABILITY, OR UNDER ANY OTHER THEORY OF LIABILITY, EXCEED IN THE AGGREGATE THREE MILLION U.S. DOLLARS ($3,000,000). THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM DEEPWATCH'S GROSS NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

8.2 Commencement of Actions; Dispute/Mitigation of Damages.

(a) No Party may commence any action under this MSA or any Order Form more than six (6) years or the shortest time permitted by law, after the occurrence of the breach or event giving rise to the claim for damages and/or indemnification.

(b) When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, and to the extent required access to Customer Third Party Software and

data is still being provided and available, Deepwatch shall proceed diligently with performance of Services under the Order Form and terms of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

(c) The claiming Party shall promptly use commercially reasonable efforts to mitigate and avoid any damages.

9. Term; Termination

9.1 Term.

The term of this MSA commences on the Effective Date and remains in effect until (i) otherwise terminated or (ii) all Order Forms have expired or been terminated.

9.2 Termination.

Customer shall use best efforts to communicate to Deepwatch its intent to terminate this MSA or any Order Form by sending at least ten (10) days prior written notice to Deepwatch Attn: Legal to 7800 East Union Avenue, Suite 900, Denver, Colorado 80237 with a cc to legal.Deepwatch.com indicating "Termination Notice" in the subject line.

9.3 Effect of Termination.

Upon any termination of this MSA or any Order Form for any reason, Customer shall, as of the date of such termination, immediately cease accessing and otherwise utilizing the Services (except as permitted under Section 9.4) and any Deepwatch Confidential Information. If Customer terminates this MSA or any Order Form prior to the expiration of the Subscription Term then in effect, Customer shall be entitled to a pro-rata refund from Deepwatch or the Reseller of all pre-paid Fees for the Services paid for by Customer but not provided by Deepwatch beyond the effective date of termination.

9.4 Retrieval of Customer Data.

If Deepwatch receives a written request from Customer within thirty (30) days after any expiration or termination of this MSA or applicable Order Form, then for a period of up to thirty (30) days after such written request is received, Deepwatch will make the Customer Data available to Customer at no additional cost through the Services on a limited basis for the sole purpose of allowing Customer to retrieve such Customer Data. After such thirty (30) day period for retrieval of Customer Data has elapsed, Deepwatch will have no obligation to maintain or provide any Customer Data and may thereafter, unless prohibited by Law, delete all Customer Data without further obligation or any liability to Customer or any third party for such deletion. If Customer requires Deepwatch's assistance, Customer may purchase Professional Services from Deepwatch or the Reseller at such entity's then-current billing rate pursuant to a written Order Form or Statement of Work entered into in accordance with such terms. With respect to each Party's Confidential Information (subject to Section 5.3 and other than Customer Data covered by the terms in this Section 9.4), upon receipt of a written request from the other Party within thirty (30) days after any expiration or termination of this MSA, each Party will promptly return the other Party's Confidential Information or destroy such Confidential Information within such Party's direct possession and provide written confirmation of such destruction; provided, however, that Deepwatch will not be obligated to destroy or erase Customer's Confidential Information that may be contained in any archived data storage.

9.5 Transition Services.

In the event that this Agreement or any applicable Order Form is terminated by Deepwatch for any reason other than non- payment or material breach of the terms of the by Customer, upon written request by Customer provided within ten (10) business days following notice of termination, Deepwatch shall provide transition services for a period of no longer than three

(3) months after the relevant Subscription Term at Deepwatch's then-current billing rates (the "Transition Services") to assist Customer to transition from Deepwatch to such other vendor as Customer believes will be required by Customer to continue its business. As part of the Transition Services, Deepwatch shall, following a written request by Customer, provide Customer with documentation and assistance to the extent that such documentation is of a non-confidential nature and generally made available to former clients transitioning to another vendor, and any other relevant technical information that may be reasonably requested by Customer pursuant to the above restrictions. Deepwatch and Customer shall provide commercially reasonable cooperation to one another while the Transition Services are being provided and both parties shall endeavor to complete the Transition Services as promptly as possible.

10. General Provisions

10.1 Export and OFAC Compliance.

The Services and other technology made available by Deepwatch, and all derivatives thereof, may be subject to export laws and regulations of the United States and other jurisdictions. Each Party represents that neither it nor any of its employees is (a) a person or entity with whom U.S. entities are restricted from doing business under regulations of the Office of Foreign Asset Control ("OFAC") of the Department of the Treasury (including those named on OFAC's Specially Designated and Blocked Persons List) or under any statute, executive order, or other governmental action; or (b) named on any U.S. government denied-party list. Customer shall not permit any Users to access or use any of the Services in a U.S. embargoed country or in violation of any U.S. export law or regulation.

10.2 Employee Solicitation.

While this MSA is in effect and for one (1) year thereafter, Customer shall not, directly or indirectly, solicit for employment or engage (whether as an employee, independent contractor, or consultant) any Deepwatch employee or subcontractor who was directly involved in providing any of the Services or Professional Services. An employee's or subcontractor's response to a general, non-targeted advertisement for employment shall not be deemed a solicitation for the purposes of this MSA.

10.3 Survival.

The first paragraph of this MSA and Sections 1, 2.1, 2.3(e), 2.3(f), 2.3(g),and 3 through 10 as well as all provisions of this MSA (including each Order Form) relating to disclaimers of warranties, remedies, damages, liability, confidentiality, payment obligations, restrictions on use, and any other terms that either expressly or by their nature should survive, shall survive any expiration or termination of this MSA for any reason, and shall continue in full force and effect.

10.4 Publicity.

Neither Party may issue any press release regarding this MSA without the other Party's prior written consent. Either Party may include the other Party's name in customer or vendor lists, subject to and in accordance with the other Party's standard guidelines.

10.5 Entire Agreement; Interpretation; Order of Precedence.

This MSA is the entire agreement between Customer and Deepwatch regarding Customer's use of Services and supersedes and merges all prior and contemporaneous, agreements (including, without limitation, any confidentiality or non-disclosure agreement entered into between the Parties), understandings, proposals, marketing materials, and representations, whether written or verbal, concerning its subject matter and the Services and there are no representations, understandings, or agreements that are not fully expressed in this MSA. Except as otherwise provided herein, no provision of this MSA (including any Order Form) may be amended, modified, superseded, or terminated, or any term or condition waived, unless the Parties (or, with respect to an Order Form, the Reseller) agree in writing, signed by a duly authorized representative of each Party (or, with respect to an Order Form, the Reseller). The Parties agree that any term or condition stated in any Customer purchase order or any other Customer ordering documentation is inapplicable and void. This MSA (including each Order Form) will be construed and interpreted fairly, in accordance with the plain meaning of its terms, and there will be no presumption or inference against the party drafting this MSA or any Order Form in construing or interpreting any of the provisions. Headings contained in this MSA are inserted for convenience of reference only and shall not in any way define or affect the meaning or interpretation of any provision of this MSA. Terms for which meanings are defined in this MSA shall apply equally to the singular and plural forms of the terms defined. Unless otherwise indicated, in this MSA, (a) "including"

(i) shall mean "including, without limitation" or words of similar effect; and (ii) when used in one instance to specify the inclusion of a particular term or meaning within another term or meaning shall not operate to exclude such specified term or meaning from the other term or meaning in instances where similar inclusive language does not appear; and (b) "or" connotes any combination of all or any of the items listed. In the event of any conflict or inconsistency between or among the documents, the following order of precedence shall be: (a) the applicable Order Form; (b) this MSA; and (c) the Documentation.

10.6 Assignment.

Neither Party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the
other Party's prior written consent (not to be unreasonably delayed or withheld).

10.7 Relationship of the Parties; Third Party Beneficiaries.

The Parties are independent contractors. This MSA does not create any partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties. Customer further

acknowledges and agrees that, in order to provide certain types of service(s) to Customer from time to time Deepwatch will upon written direction from Customer (email accepted) and on Customer's behalf and in Customer's name, enter into third party contracts and/or accept the terms and conditions of third party supplier EULA(s) and/or subscription agreements. Customer acknowledges and agrees that, upon Deepwatch's acceptance of the terms and conditions of any EULA on Customer's behalf for the use of any software or service, the third party licensor and/or service provider will have the right (and will be deemed to have accepted the right) to enforce the EULA against Customer as a third party beneficiary. Nothing else in this MSA, express or implied, is intended to confer on any person or entity any rights or remedies in or by reason of this MSA.

10.8 Force Majeure.

(a) Excusable delays shall be governed by FAR 552.212-4(f).

(b) Notwithstanding anything to the contrary, Customer acknowledges Deepwatch subscription services are provided remotely and service disruptions involving hardware, software, or power systems not within such Party's possession or beyond its reasonable control or any denial of service attacks shall be deemed an unforeseen occurrence beyond the reasonable control of Deepwatch and without its fault or negligence.

10.9 Waiver.

No failure or delay by either Party in exercising any right or remedy under this MSA will constitute a waiver of that right or any other right. Any waiver of any right or remedy under this MSA must be in writing and signed by a duly authorized representative of each Party. A waiver on one occasion shall not be construed as a waiver of any right or remedy on any future occasion. Except as otherwise expressly stated in this MSA, the remedies provided in this MSA are in addition to, and not exclusive of, any other rights and remedies of a Party at law or in equity.

10.10 Governing Law; Venue.

This MSA and any claim, controversy, right, obligation or dispute arising under or related to this MSA shall be governed by and construed in accordance with the Federal laws of the USA, without regard to conflicts of laws principles. The Parties agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods do not apply to this MSA. THE PARTIES HEREBY WAIVE ANY RIGHT TO TRIAL BY JURY IN CONNECTION WITH ANY ACTION, PROCEEDING, OR COUNTERCLAIM BROUGHT BY EITHER PARTY AGAINST THE OTHER PARTY ON ANY MATTER WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THIS MSA OR ANY ORDER FORM.

This Agreement may be executed and delivered in any number of counterparts by facsimile, emailed PDF, or electronic signature, each of which will be deemed an original, but all of which together will constitute one and the same instrument.

10.11 Notices.

All notices (except for routine business communications, e.g., maintenance windows, scheduling of meetings) shall be in writing and sent via certified or registered mail, return receipt requested, or by overnight courier service. All notices to Deepwatch shall be addressed to the Chief Financial Officer, with a copy to the Legal Department, and sent to Deepwatch, Inc., 8116 Arlington Blvd., Suite 252, Falls Church, Virginia 22042. Notices to Customer shall be addressed to Customer's signatory and sent to Customer's address provided below.

10.12 Severability.

If any provision of this MSA is held by a court of competent jurisdiction to be unenforceable and/or contrary to Law, the provision will be deemed null and void, and the remaining provisions of this MSA will remain in full force and effect.

10.13 Customer Reference.

Deepwatch may also list Customer's name on a client list, which is provided to prospective customers to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

10.14 Insurance

(a) For the Term of this Agreement, Deepwatch shall at its own cost and expense maintain one or more insurance policies with the following coverage limits during the Subscription Term with at least the following limits:

(i) Workers' Compensation insurance in accordance with statutory and regulatory requirements, with coverage limits of not less than $1,000,000 per occurrence
(ii) Commercial General Liability insurance coverage limits of not less than $1,000,000 per occurrence, $2,000,000 aggregate
(iii) Umbrella Liability insurance coverage limits of not less than $5,000,000 per occurrence, $5,000,000 aggregate
(iv) Errors and Omissions insurance coverage limits of not less than$1,000,000 per occurrence, $2,000,000 aggregate
(v) Cyber Liability insurance coverage limits of not less than $5,000,000

(b) Deepwatch shall provide upon request a certificate of insurance evidencing all the insurance coverages provided under this section.

(c) Deepwatch will provide written notice if its insurance under such policies will be cancelled or materially changed within thirty (30) days.

EXHIBIT A
DEEPWATCH FEDERAL SERVICE LEVEL AGREEMENT
Version: 2022 05 02

Overview

This Service Level Agreement (SLA) document is provided for customers as referenced in the Agreement. Any capitalized terms not defined herein shall have the same meanings assigned in the Agreement.

Service Level Agreements

Uptime Service Availability Commitment SLA

During the term of an Order Form, the Deepwatch infrastructure and software platform will be available no less than 99.9% of the total number of minutes within each calendar month.

Initial Response and Update SLA

Impact	Service Request*	Operations Incident*	Threat Event	Validated Security Incident	SLA
Critical	N/A	1 Hour	N/A	1 Hour	95%
High	1 Business Day	1 Business Day	N/A	2 Hours	95%
Medium	3 Business Days	3 Business Days	N/A	8 Hours	95%
Low	5 Business Days	5 Business Days	N/A	24 Hours	95%
Informational	N/A	N/A	N/A	N/A	N/A

** Applicable to Service Requests and Operations Incidents for standard and normal changes*

Deepwatch applies the Initial Response and Update SLA to validated incidents. Deepwatch only provides measurements and reporting on the handling of threat events and unvalidated incidents. The Initial Response and Update SLAs also do not apply during the initial sixty (60) days of onboarding or adding any additional division or business unit.

Resolution SLA

Customer agrees that this SLA does not apply to the resolution of any incident but only to the provision of initial response and updates.

Carve-Outs and Credits

SLA Credits

Any request for a credit must be in writing and received by Deepwatch within fifteen (15) days following the last day of the month of Deepwatch's failure to meet any of its SLA commitments in a calendar month. Upon receipt of such a written request and verification by Deepwatch, Deepwatch will issue a credit of 1/30th of the monthly subscription fee for the affected Service for the month of the failure. If a written request is not received within fifteen (15) days following the last day of the month of the failure, Customer's right to receive a service credit with respect to the month in which Deepwatch failed to meet its SLA commitment shall be waived.

Customer Requirements

In order for the SLAs to apply, Customer must submit the case through the customer portal.

Reproducing Errors

Deepwatch must be able to reproduce errors with an unmodified version of the Services being accessed in order to resolve them. Customer agrees to cooperate and work closely with Deepwatch to reproduce errors, including conducting diagnostic or troubleshooting activities as reasonably requested.

Exclusions

In determining whether Deepwatch has met its SLA commitments, the following exclusions shall apply with respect to Deepwatch's obligation to provide support under the specific care plan which Customer selected and if Customer might be eligible for a service credit: (i) if Customer breaches any of its obligations with Deepwatch, including payment obligations; (ii) any Deepwatch scheduled maintenance; (iii) any Service unavailability due to any force majeure event or any other factor outside of Deepwatch's reasonable control including but not limited to telecommunications or internet problems, power failures, and/or service provider failures outside of Deepwatch's data center; (iv) any problem resulting from any hardware, software, infrastructure and/or platforms not provided by Deepwatch or any third party's acts, errors or omissions ; (v) any interruption or unavailability resulting from Customer's use of the Services in an unauthorized or unlawful manner or any interruption resulting from the misuse or improper use of the Services; (vi) any Service Requests and/or Operational Incidents, as defined below, related to non-standard changes; (vii) any interruption resulting from disconnection or suspension of the Services for Customer's non-payment in a timely manner of any Deepwatch invoice; and (ix) any industry wide security threat (e.g., WannaCry). The service credit remedy set forth in this SLA is the Customer's sole and exclusive remedy for the unavailability of any applicable Services in the Order Form. Under no circumstance, shall Deepwatch's failure to meet an SLA commitment be deemed a default or breach under the Agreement. All SLAs for Cases will be delayed while Deepwatch is waiting on Customer or third- party vendor's action or information while the Case status is in a "waiting on the customer," "waiting on a third party" or "pending other prerequisites" status. Uptime SLAs do not apply for planned

maintenance including unexpected outages resulting from planned maintenance where the Customer has not invested in high availability.

Additional Conditions

Deepwatch makes no guarantee that breaches, compromises or unauthorized activity will not occur across a customer's network or IT environment.

Key Terms

Where practicable, Deepwatch bases key terms in NIST and ITIL definitions.

Case Types

- Operations Incident - An unplanned interruption to service or reduction in the quality of service. An unrealized but imminent threat to interrupt or reduce the quality of service is also an Operations Incident. Operations Incidents may be linked to a change record as part of resolving the incident.
- Service Request - A formal request from a Customer for something to be provided. Service requests may be linked to a change record as part of fulfilling the request.
- Threat Event - An event or situation that has the potential for causing undesirable consequences or impact.
- Security Incident - A threat event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
- Change - An adjustment to a system that may arise reactively in response to an Operations Incident, proactively from a Service Request, or from service enhancement initiatives.

Change Management

- Change Management - A set of standard operating procedures for changes to include change review and approval requirements and change windows for the varying types of changes.
- Standard Change - A pre-authorized change that is lower risk, relatively common and follows a defined procedure. Standard changes do not adhere to change management and they are logged and tracked using the Service Request or Incident driving the need for the change.
- Normal Change - A change that is higher risk, relatively common and follows a defined procedure. Normal changes adhere to change management and are logged and tracked in a change record separate from the Service Request or Incident driving the need for the change.
- Emergency Change - A change required to resolve a critical Operations Incident. If a normal or non-standard change, the change will adhere to change management immediately following the change but not to impede resolving the incident.

- Non-standard Change - A change that has unknown risk because it is not common and does not follow a predefined procedure. Non-standard changes adhere to change management.

Change Examples

Change Type	Service Request	Operations Incident
Standard	• Initial deployment of or enhancement to a Security Information Event and Management (SIEM) log source or use case pre-built by Deepwatch or SIEM vendor and is Splunk Common Information Model (CIM) compliant • Integration between a Deepwatch platform and the same platform within the Customer environment • Creation, modification, or deletion of a firewall rule • Creation, modification, or deletion of a vulnerability report	• An inoperable or malfunctioning SIEM log source or use case pre-built by Deepwatch or SIEM vendor and is CIM compliant • An inoperable or malfunctioning integration between a Deepwatch platform and the same platform within the customer environment • A down or inoperable platform managed by Deepwatch
Normal	• A planned upgrade of a platform to the latest patch or release certified by Deepwatch • Decommissioning of a platform managed by Deepwatch	• Applying a platform patch or new release certified by Deepwatch to resolve a non-critical Operations Incident
Emergency	• N/A	• Any standard or normal change required to resolve a critical Operations or Security Incident
Non-standard	• Initial deployment or enhancement to a SIEM log source or use case, not pre-built by Deepwatch or SIEM vendor and is not CIM compliant	• An inoperable or malfunctioning SIEM log source or use case, not pre-built by Deepwatch or SIEM vendor and is not CIM compliant • An inoperable or malfunctioning integration between a Deepwatch platform and a different platform within the customer environment

Change Type	Service Request	Operations Incident
Out of Scope	Cases not driven by cybersecurity value or not achievable within the software platform Deepwatch manages	

Prioritization

- Priority - A classification used to identify the relative importance of a case. Priority is based on impact and urgency relative to the Deepwatch service.
- Impact - A measure of how service levels will be affected as a result of the case. The impact may be the result of fulfilling the case or a result of not fulfilling the case.
- Urgency - A measure of how long until the case has an impact on the service level.
- Business Urgency - A measure of how long until the case has an impact on the Customer's business operations. Deepwatch will make reasonable attempts to expedite cases based on Customer business urgency but business urgency does not influence case prioritization or the SLA.

Prioritization Examples

Prioritization	Service Request	Operations Incident	Security Incident
Critical	• N/A	• Correcting a SIEM log source and use case from the Deepwatch maturity model that collectively are not parsing or producing threat events as intended • Restoring a platform that is unavailable or inoperable • Creation or modification of a firewall rule as needed to mitigate a critical security incident • Creation, modification, or execution of a vulnerability scan and report as needed to manage a critical threat event	• An unauthorized actor (human or automated) is present in the environment • Leakage or exposure of sensitive information • The platform is unavailable or inoperable to provide the intended security function • SIEM log source from Deepwatch maturity model is not reporting in or not parsing correctly and is associated with an active use case from the Deepwatch maturity

Prioritization	Service Request	Operations Incident	Security Incident
			model.
High	• A planned upgrade of a platform to the latest patch or release certified by Deepwatch • Initial deployment of a log source and associated use cases from within the Deepwatch Maturity Model	• Applying a platform patch or new release certified by Deepwatch to resolve a non-critical Operations Incident • Platform performance is degraded but the intended security function remains operable • Creation, modification, or execution of a vulnerability scan and report as needed to manage a high-security incident • Creation or modification of a firewall rule as needed to mitigate a high-security incident	• Sudden decrease or increase in data ingested from log source within Deepwatch"s maturity model • Suspicious activity potentially indicative of an unauthorized actor (human or automated) being present in the environment or possible leakage or exposure of sensitive information

Prioritization	Service Request	Operations Incident	Security Incident
Medium	• Initial deployment of a log source and associated use cases provided by the SIEM vendor and CIM compliant • Malicious IP event [host scanning] • Vulnerability report creation or modification • FW rule creation, modification, or deletion	• Correcting a SIEM log source or use case provided by the SIEM vendor that is CIM compliant and not parsing or producing threat events as intended • Creation, modification, or execution of a vulnerability scan or report as needed to manage a medium security incident. • Creation or modification of a firewall rule as needed to mitigate a medium security incident	• Reconnaissance activity such as port scanning, excessive failed logins, or outbound traffic to known bad actors
Low	• Initial deployment of a log source and associated use cases requiring customized development	• Correcting a SIEM log source or use case customized for an individual customer by Deepwatch that is not parsing or producing threat events as intended • Creation, modification, or execution of a vulnerability scan or report as needed to manage a low-security incident	• Threat activity that is mitigated such as via a firewall block but requires reporting for regulatory compliance or other reasons

Prioritization	Service Request	Operations Incident	Security Incident
		• Creation or modification of a firewall rule as needed to mitigate a low-security incident	
Informational	• Request for documentation related to how Deepwatch operates	• N/A	• Threat event reports as required for regulatory compliance or other need to review high volumes of threat events • Initial threat hunt before the hunt reveals a security incident

Deepwatch tailors prioritization of threat events for each Customer's risk tolerance and regulatory requirements and therefore threat events are not represented in the above table. Deepwatch bases SLAs on impact as defined in this document and Deepwatch retains the right to reclassify the impact and resulting SLA on a case per the definitions above.

Deepwatch may make updates to this SLA from time to time in Deepwatch's sole discretion so long so long as such updates do not materially reduce either the service levels provided to Customer or the remedies available to Customer. Any such changes will apply only on a prospective basis from the effective date of such change. Deepwatch may also update the toll-free telephone number and/or trouble ticket contacts or procedures by providing Customer with written notice.

Fortress Government Solutions

FORTRESS GOVERNMENT SOLUTIONS END USER LICENSE AGREEMENT

This End User License Agreement ("Agreement") by and between Fortress Government Solutions LLC ("Fortress") and Ordering Activity under GSA Schedule contracts identified in the Purchase Order ("Client"). This Agreement sets forth the terms and conditions applicable to the license of certain Fortress software and data.

1. Definitions.

a. **"Client Software"** means the software provided by Fortress for installation locally, or via any online interface, by Client.

b. **"Content"** means any data or content that is provided or uploaded by Client for transmission, storage, integration, import, display, distribution, or use in or through the Products.

c. **"Data"** means recorded information of any kind regardless of the form or method of recording that is hosted or provided by Fortress through the Client Software or otherwise under the Order.

d. **"Order"** means the order through which Client obtains a license or access right to certain Fortress commercial computer software products or contracts for certain services from Fortress.

e. **"Product(s)"** means the Client Software, Data, and Software specified in the Order.

f. **"Software"** means the Fortress proprietary commercial computer software, models, and algorithms, and any helpers, extensions, plug-ins, and add-ons, in any format, specified in the Order (and any related purchase orders, statements of work, or amendments, which are incorporated by reference herein) or provided in connection with this Agreement, any third-party software incorporated therein or in the Client Software, and any improvements, modifications, derivative works, patches, Updates, and upgrades thereto that Fortress provides in its discretion to Client hereunder.

g. **"Updates"** means Product changes that Fortress in its discretion implements in the generally available Products specified in the Order. Updates do not include platform capabilities, configurations, or modules not specified in the Order that Fortress makes available for an additional charge.

2. Term and Termination. This Agreement shall begin and remain effective for the period of time specified in the Order ("Term") either (i) in perpetuity if the Order specifies a perpetual license, or (ii) for the number months or years set forth in the Order if the Order specifies a term licenses, unless otherwise terminated as provided herein. During the Term, this Agreement may be terminated by Client for convenience in accordance with the Federal Acquisition Regulation ("FAR") termination for convenience clause552.212-4(l).

3. Limited License to Software. Subject to Client's compliance with this Agreement, Fortress grants to each Client individually a non-transferable, non-assignable, non-exclusive, limited license without any right to sublicense or share with Client-related entities during the Term to install, execute, and use the Software in object code format solely for Client's internal purposes as specified in the Order and in accordance with the technical specifications provided by Fortress. This license is not fungible and shall not be reallocated or expanded by Client for any purpose not specified in the Order, and the license may not be shared among separate governmental departments or agencies unless otherwise specified in the Order.

4. Limited License to Data. Subject to Client's compliance with this Agreement, Fortress grants to each Client individually a non-transferable, non-assignable, non-exclusive, limited license without any right to sublicense or share with Client-related entities during the Term to use the Data solely for Client's internal purposes as specified in the Order and in accordance with the technical specifications provided by Fortress, and the license may not be shared among separate governmental departments or agencies unless otherwise specified in the Order. This license is not fungible and shall not be reallocated or expanded by Client for any purpose not specified in the Order. Client and Client's contractors, employees, or others given access to Data may not take and share any Data externally in any form, including but not limited to taking excerpts or portions of any Data to include in any externally shared documentation, marketing materials, reports, or any other externally distributed materials.

5. Ownership of Intellectual Property. Client acknowledges and agrees that the Software, Data, Products, Updates, and any other related documents, materials, or information provided by Fortress, are and shall remain the sole and exclusive property of Fortress, and all right, title and interest therein shall remain with Fortress including any intellectual or industrial property interests or rights in any trademark, copyright, or patent of the foregoing ("Intellectual Property"). No ownership rights are being conveyed to Client under this Agreement. Unless otherwise agreed to in writing by Fortress, nothing in this or any other agreement or in the course of dealing between Fortress and Client shall be construed to grant to Client any ownership right, title or interest in or license to any of the Intellectual Property. Except for the express rights granted herein, Fortress does not grant any other licenses, whether express or implied, to any Fortress software, services, technology, or intellectual property. Client shall maintain and not remove, obscure, or alter any intellectual property notices, trademarks, logos, tradenames, or other identifiers or notices that appear on any materials, documentation, software, data, or intellectual property of Fortress. The provisions of this section shall survive expiration or termination of this Agreement for any reason.

6. Restrictions on Use of Intellectual Property. Client shall not, and shall not allow any third party to infringe upon Fortress's Intellectual Property. Client shall require any of Client's contractors or employees to agree to the terms of this Agreement, and shall be responsible for ensuring Client's contractors and employee's compliance with this Agreement. Client shall not, and shall not allow any third party to (i) decompile, disassemble, scan, reverse engineer, or attempt to discover any source code, underlying ideas, algorithms, or other data of any Products (except to the extent applicable law

expressly prohibits such a restriction); (ii) provide, lease, lend, use for timesharing or service bureau purposes, or otherwise use or allow others to use a Product for the benefit of any third party; (iii) list or otherwise display, copy, or reuse any code of any Product; (iv) copy any Products or components thereof, except where Client is hosting is specified then Client may make a reasonable number of copies of the Software as well as related documentation solely for backup, archival or disaster recovery purposes; (v) develop any improvement, modification, or derivative work of the Products or include a portion thereof in any equipment or item; (vi) allow the transfer, transmission, public communication, export, or re-export of any Intellectual Property or any portion thereof; (vii) conduct performance, benchmark, or other testing or technical evaluations of the Products without prior written consent from Fortress; (viii) gain or attempt to gain unauthorized access to the Products, or any element thereof, or circumvent or otherwise interfere any authentication or security measure of the Products; (ix) interfere with or disrupt the integrity or performance of the Products; (x) input, upload, transmit, or otherwise provide material containing software viruses or other harmful or deleterious computer code, files, scripts, agents, or programs, to or through the Products, or; (xi) use, evaluate or view Intellectual Property for the purpose of developing, designing, modifying, or otherwise creating any environment, software, models, algorithms, products, program, or infrastructure or any portion thereof, which performs functions similar to the functions performed by the Products.

7. Permitted Use of Intellectual Property. Client may use the Intellectual Property for the purpose identified in the Order subject to the limited license granted herein. Fortress may provide portions of the Products with notices and open source licenses from communities and third parties that govern the use of those portions. Client may use such portions subject to the obligations Client may have under such open source license and this Agreement shall not alter any such obligation; however, the disclaimer of warranty and limitation of liability provisions in this Agreement shall apply to all Products, including opensource materials.

8. Ownership of Content. Client retains all rights, title, and interest in and to the Content, other than providing Fortress with a non-transferable, non-assignable, non-exclusive, limited license without any right to sublicense during the Term to utilize the Content to compile usage statistics, include in Fortress' databases associated with threat intelligence, or otherwise to use for Fortress' internal purposes.

9. Authorized User Accounts. Client may establish Product accounts in an amount not exceeding that set forth in any current Orders ("Accounts") for Client's employees or independent contracts with a need to access the Products on behalf of Client ("Authorized Users"), on the condition that Customer has confidentiality obligations in place for each Authorized User at least as restrictive as the ones stated herein. Upon request of Fortress, Client shall provide Fortress with the company names of any independent contractors who have access to the Products. Client shall provide access only to Authorized Users, request such Authorized Users to keep Account login information, including user names and passwords, strictly confidential and not provide such Account login information to any unauthorized parties, and to use standard security measures to protect Accounts including but not limited to multi-factor authentication. Client shall be responsible for monitoring and controlling access to the Products

and Accounts and maintaining the confidentiality of Account login information. Client shall immediately deactivate any compromised Account or change the Account's login information as appropriate. Client shall inform each Authorized User of its obligations hereunder and ensure that each Authorized User at all times abides by the terms of this Agreement. Client shall immediately notify Fortress in the event Client or an Authorized User becomes aware of any violation of the terms of this Agreement, including any breach of Confidential Information. Client is solely responsible for any use of the Products that occurs on Client's Accounts and shall be liable for any breach of this Agreement by an Authorized User. Client shall be responsible for authorizing and protecting Accounts.

10. Permitted Analytics. Fortress may collect analytics, statistics, metrics, or other data related to Client's use of the Products in order to provide the Products to Client, for statistical use of non-personally identifying information, or to monitor, analyze, maintain and improve the Products. Fortress retains all rights, title, and interest in any resulting data or materials.

11. Third Party Service. Fortress may utilize or make available third-party services in the provision of the Products. Fortress is not responsible or liable for any third party services.

12. Product Support. Fortress shall provide Client with professional services related to the Products specified in the Order and may provide additional services with respect to Client's use of the Products upon request and mutual written agreement of the parties. Subject to payment of the applicable fees in the Order, Fortress shall (i) use commercial reasonable efforts to provide Client with product support and Updates in accordance with and subject to Fortress's standard support and maintenance terms and conditions and as specified in the Order; and (ii) provide training services as specified in the Order. Any renewal to the Order for support, maintenance, or training must be made in full and failure to pay by the end of the period specified in the Order shall be deemed to be a cancellation of the foregoing features. Client may reinstate such services provided Fortress offers the services and Client pays the current GSA Pricelist fee and any fees that would have been payable during the period the services were cancelled. Fees shall be negotiated by Fortress and Client. In the event of cancellation and reinstatement, fees shall default to the standard undiscounted rate available to customers via Fortress's GSA Schedule or other applicable commercial schedule. Fortress shall have the right to update the Products from time to time with improvements or modifications to a previously purchased capability or module or to otherwise improve functionality of the Productions. Fortress may deliver the updates electronically.

13. Confidentiality. Fortress may disclose, or Client may have access to, certain financial, technical, legal, marketing, network, and other business information, reports, records, or data (including, but not limited to, PII, computer programs, code, systems, applications, analyses, passwords, procedures, output, information regarding software, sales data, vendor lists, customer lists, and other customer-related information, business strategies, advertising and promotional plans, creative concepts, specifications, designs, drawings, documents or other material) which Fortress deems, and Client should consider, proprietary or confidential (and of independent economic value) to Fortress ("Confidential Information"). Confidential Information shall also include the Data, Software, Products, business

methods, security evaluation techniques and reporting, software, and pre-existing proprietary materials licensed or provided to, or accessed by, Client. To the extent allowed under applicable law, Client shall treat all Confidential Information provided by Fortress pursuant to this Agreement and any Order as proprietary and confidential, and Client shall not (without the prior written consent of Fortress) disclose or permit disclosure of such Confidential Information to any third party, provided that Client may disclose, on a need-to- know basis, such Confidential Information to its third party subcontractors who have signed non- disclosure agreements with Client, and to current employees, officers, or directors, or legal or financial representatives. Client shall safeguard all Confidential Information of with at least the same degree of care (which in no event shall be less than reasonable care) as Client uses to protect its own confidential information. Client shall use Confidential Information solely for the purpose of fulfilling the purpose specified in the Order. Client shall not to use or disclose Confidential Information for its own benefit or for the benefit of others, except as otherwise required by law or authorized by this Agreement, the applicable Order, or Fortress in writing. Notwithstanding the foregoing, the parties agree that the following information shall not be deemed Confidential Information, and Client shall have no obligation with respect to any such information: (i) information which is independently developed by Client without any breach of this Agreement by Client, and which can be shown by documentary evidence; (ii) information which is or becomes in the public domain by no fault or wrongful act of Client; (iii) information which is known by Client prior to disclosure by Fortress; (iv) information which is disclosed to Client by third party who was not under a similar restriction or obligation of confidentiality to the disclosing party, and without breach of this Agreement; (v) information which is approved for release by written authorization of Fortress and the third party owner of the disclosed information; or (vi) information which is disclosed pursuant to the lawful requirement or order of a court or governmental agency, provided that, upon Client's receipt of a request for such a disclosure, Client gives prompt notice thereof to Fortress (unless such notice is not possible under the circumstances) so that Fortress may have the opportunity to intervene and contest such disclosure and to seek a protective order or other appropriate remedy. Fortress recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor. All Confidential Information transmitted or disclosed hereunder will be and remain the property of Fortress, and Client shall (at Fortress's election) promptly destroy or return to Fortress any and all copies thereof (1) upon termination or expiration of this Agreement, the applicable Order, or both, or (2) upon the written request of Fortress. Upon the request of Fortress, any such destruction shall be certified in writing by Client. Client is responsible for any breaches of this section by its employees, independent contractors, agents, or other persons to whom Confidential Information was disclosed. The provisions of this section shall survive expiration or termination of this Agreement for any reason.

14. Payment and Delivery. Client shall pay Fortress as set forth in the Order. Payment shall be made in the currency and method specified in the Order. Payment shall be made in the currency and method, and within the timeframe, specified in the Order. Any late payments shall be subject to the U.S. Prompt Payment Act. Products are deemed delivered upon being made available to Client.

15. Government Matters. The Products and related services, support and maintenance, and training are “commercial products”, “commercial services”, and “commercial computer software” as defined under 48 CFR 2.101. If the Client is a Department of Defense agency, the Client Software constitutes “commercial computer software” as defined in paragraph (a)(1) of the Department of Defense FAR Supplement (“DFARS”) clause 252.227-7014, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation. If Client or end user is a U.S. governmental entity, Client acknowledges and agrees that (i) use, duplication, reproduction, release, modification, disclosure, or transfer of the Products or related Intellectual Property, documents, or materials shall be subject to FAR 12.211 and FAR 12.212, (ii) the Products and Intellectual Property were developed exclusively at private expense, and (iii) all other use of the Products or Intellectual Property except in accordance with the license and rights granted herein is strictly prohibited. Notwithstanding anything to the contrary, the terms and conditions describing the Government’s use and rights are in lieu of, and supersede, any conflicting provisions that address Government rights in the Products or Intellectual Property that may be incorporated in any contract or subcontract under which the Products are accessed or licensed.

16. Indemnification. Fortress shall have the right to intervene to defend, indemnify, and hold harmless Client from any against damages, costs, and reasonable attorneys’ fees arising out of any claim of infringement or violation of any U.S. patent, copyright, or trademark asserted against Client by a third party based on Client’s use of the Products in accordance with this Agreement provided that Client notifies Fortress of such claim withing twenty (20) days of receipt, reasonably cooperates with Fortress, and agrees that Fortress shall have the right to control and direct the investigation, defense, and settlement of such claim. If Client’s use of the Products is, or in Fortress’s opinion is likely to be, enjoined then Fortress may at its sole discretion (i) provide a substantially functionally similar substitute to the Products, (ii) procure for Client the right to use the Products, or (ii) submit a claim to Ordering Activity Contracting Officer under the Contracts Dispute Act to terminate this Agreement and refund to Client as appropriate and prorated for the remaining portion of the Term as of the effective date of termination. The foregoing indemnification obligation of Fortress shall not apply: (1) if the Products are modified by any party other than Fortress or modified at Client’s request, but only to the extent the alleged infringement would not have occurred but for such modification; (2) if the Products are combined with any non-Fortress products or processes not authorized by Fortress, but only to the extent the alleged infringement would not have occurred but for such combination; (3) to any unauthorized use of the Products; (4) to any superseded release of the Products if the infringement would have been avoided by the use of a current release of the Products that Fortress provided to Client prior to the date of alleged infringement; or (5) to any third party products, software, or services contained within or used to deliver the products. THIS SECTION SETS FORTH FORTRESS’S SOLE LIABILTIY AND CLIENT’S SOLE AND EXCLUSIVE REMDEDY WITH RESPONSE TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice’s right to defend any claim or suit brought against the U.S. pursuant to 28 U.S.C. § 516.

17. Limited Warranty. Fortress shall provide all goods and services in a good and workmanlike manner.

18. Disclaimer. ALL SALES ARE FINAL AND NO PURCHASES OF PRODUCTS ARE EXCHANGEABLE, OR OFFSETTABLE EXCEPT AS EXPRESSLY SET FORTH IN THE LIMITED WARRANTY. FORTRESS WARRANTS THAT THE PRODUCTS WILL, FOR A PERIOD OF SIXTY (60) DAYS FROM THE DATE OF YOUR RECEIPT, PERFORM SUBSTANTIALLY IN ACCORDANCE WITH PRODUCTS WRITTEN MATERIALS ACCOMPANYING IT. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, FORTRESS MAKES NO WARRANTIES WITH RESPECT TO THE PRODUCTS, AND SUCH PRODUCTS ARE PROVIDED "AS IS." FORTRESS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, SPECIFICALLY, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR OF NON- INFRINGEMENT. FORTRESS DOES NOT WARRANT THAT THE PRODUCT WILL MEET CUSTOMER, CLIENT, OR END-USER REQUIREMENTS OR THAT THE OPERATION OF

THE PRODUCT WILL BE UNINTERRUPTED OR ERROR-FREE. FORTRESS DOES NOT CONTROL THE TRANSFER OF DATA, INFORMATION, OR CONTENT OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET OR THIRD-PARTY SERVICES, AND IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS.

19. Client Representations and Warranties. Client represents, warrants, and covenants that (i) it shall not use the Products for any unauthorized, improper, or illegal purposes; (ii) it will not transmit, store, integrate, import, display, distribution, use, or otherwise make available any Content that is or is obtained in a manner that is unauthorized, improper, or illegal; (iii) no Content infringes upon or violates any other party's rights including intellectual property rights; (iv) this Agreement imposes no obligations with respect to Content unless otherwise specified; and (iv) It has provided all necessary notifications and obtained all necessary consents, authorizations, approvals, and agreements required by any applicable laws or policies to enable Fortress to receive and process the Content.

20. Limitations of Liability. TO THE EXTENT PERMISSIBLE UNDER APPLICABLE LAW AND EXCEPT AS OTHERWISE PROVIDED FOR IN THIS AGREEMENT, FORTRESS SHALL NOT BE LIABLE UNDER THIS AGREEMENT FOR ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, STATUTORY, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS, LOSS OF USE, LOSS OF TIME, SHUTDOWN OR SLOWDOWN COSTS, INCONVENIENCE, LOSS BUSINESS OPPORTUNITIES, DAMAGE TO GOODWILL OR REPUTATION, OR OTHER ECONOMIC LOSS, REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, STRICT LIABILITY OR OTHERWISE, AND EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR SUCH DAMAGES COULD HAVE BEEN REASONABLY FORESEEN. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

21. Miscellaneous. This Agreement together with the Order(s) comprise the complete and entire agreement between the Parties with respect to the subject matter hereof. It supersedes all prior and contemporaneous oral and written agreements and discussions. This Agreement is incorporated into the Order and takes precedence over any conflicting or inconsistent provisions from whatever source,

unless expressly stated otherwise such as in the Order. This Agreement may not be amended or modified except by an instrument in writing mutually executed by both Parties. No waiver of any term or right in this Agreement shall be effective unless in writing, signed by the waiving Party. The failure of either Party to enforce any provision of this Agreement shall not be construed as a waiver or modification of such provision, or impairment of its right to enforce such provision thereafter. Neither this Agreement nor any of the licenses provided for herein may be assigned, subcontracted, or sublicensed by Client without prior written consent by Fortress. Each Party has participated in, and in any construction to be made of this Agreement shall be deemed to have participated in, the negotiating, drafting, and execution of this Agreement and each of its parts and thus shall not be construed against the drafter. All notice, report, approval, or consent given under this Agreement to shall be deemed served when deposited in the United States mail, registered or certified post, return receipt requested, with sufficient postage, or otherwise sent by a reputable delivery service with a copy via email to the addresses specified in the Order. If any provision of this Agreement shall be adjudged by any court or board of competent jurisdiction to be unenforceable or invalid, that provision shall be limited or eliminated to the minimum extent necessary to that the Agreement shall otherwise remain in full force and effect and be enforceable. Unless otherwise specified by Fortress, all products and services provided may be subject to U.S. trade controls and sanctions and may only be further exported or transported in accordance with applicable law and restrictions. It is Client's responsibility to provide Fortress with the necessary information for Fortress to comply with applicable requirements and to ensure all end-uses and end-users relating to Client's reexports and retransfers of the Products or services comply with applicable controls. This Agreement is governed by United States Federal law. The contract price excludes all state and local taxes. Fortress shall state separately on its invoices taxes excluded from the fees and Client shall pay the amount of the taxes or provide evidence necessary to sustain an exemption. Excusable delays shall be governed by FAR 552.212-4(f).

Secure Code Warrior

END USER LICENSE AGREEMENT
Commercial Subscription License and Professional Services Agreement

This Commercial Supplier Agreement and SAAS License Agreement and Services Agreement ("Agreement") is between the Customer, identified in the Purchase Order, Annex, Statement of Work, or similar document, having its principal place of business as set forth in said document, and the GSA Multiple Award Schedule (MAS) Contractor (Guidepoint Security, LLC) acting on behalf of Secure Code Warrior Inc, ("SCW" or "Company" or "Supplier") with its principal place of business at 265 Franklin Street, Suite 1702, Boston MA 02110, USA. This Agreement governs the Customer's use of the Supplier software (the "Licensed Software") and the Supplier documentation made available for use with such software. "You" or "Customer" or "Licensee" means the Government Customer (Agency) who, under GSA Schedule Contracts, is the "Ordering Activity" which is defined as "an entity authorized to order under GSA Schedule Contracts" as defined in GSA Order OGP 4800.2I, as may be amended from time to time.

1. Definitions and interpretations

1.1. The following words shall have the meaning stipulated herein below:

Affiliates means a company in which either party either wholly owns or has a controlling interest;

Applicable Data Protection Legislation means any data protection or privacy legislation which applies, respectively to the activities of the Customer and SCW, including, where applicable the European General Data Protection Regulation Act 2016 (GDPR), the UK Data Protection Act 2018, the Australian Privacy Act Cth) 1988, and any other applicable legislation

Confidential Information means any information, maintained in confidence by the disclosing Party, communicated in written or oral form, marked as proprietary, confidential or otherwise so identified, and/or any information that by its form, nature, content or mode of transmission would, to a reasonable recipient, be deemed confidential or proprietary, including, without limitation, each party, employees, business plans, methods of operation, SCW Offerings, including the SCW Learning Platform. Confidential Information will also include, without limitation:

(a) certain confidential and/ or proprietary financial, sales and distribution, marketing, research and development, organizational, technical and other business information, policies or practices, related information; and

(b) any information disclosed by a Party which relates to an actual or potential End User, vendor or third party with which the disclosing Party is in a confidential relationship

Consent means consent, permission, agreement or approval which meets the requirements for the consent of the Applicable Data Protection Legislation

Controller has the meaning as defined by Regulation (EU) 2016/679 with obligations as set forth in the regulation

Customer means the party which acquires a Subscription to the SCW Learning Platform directly or through a third party and, if applicable, End Users(s)

Defect means a defect, error or bug having a materially adverse effect on the appearance, operation or functionality of the SCW Learning Platform, but excluding any defect, error or bug caused by or arising as a result of an act or omission of the Customer, any failures of the internet or part of the internet or other mechanism designed or used to disable, erase, alter or harm the SCW Learning Platform

Device means a single personal computer, workstation, mobile phone, tablet, or other electronic devices.

Documentation means any electronic or written aids, manuals, user instructions, technical literature, training material, demo material, specifications and all other related materials, which may be accessible by the Customer in the SCW Learning Platform

End User means a person or persons employed and / or otherwise authorized by the Customer, or where applicable the Customer's group, and who is provided with a subscription by the Customer to access and use the SCW Learning Platform, and excludes any person or persons who is employed by or contracted to a competitor to Reseller and/ or SCW

Insolvency Event means a situation where in respect to either party (1) a party is unable to pay its debt as and when they fall due; (2) a receiver or administrator is appointed over the party or any part of their respective undertakings or assets; (3) a resolution for winding up the party is proposed (or ordered), with the expectation of such an order being proposed for the purpose of a bona fide reconstruction; (4) a court of competent jurisdiction makes an order to that effect; (5) it becomes subject to an order of administration; (6) it enters into any scheme of arrangement with credits or any similar process to any of the above is begun in any jurisdiction, or if it ceases or threatens to cease to carry on business

Intellectual Property means all intellectual property rights wherever in the world, whether registered or unregistered, including patents, rights to any invention, copyrights and related rights, moral rights, rights in computer software, trade marks, service marks, trade names, domain names, rights in any goodwill and the right to sue for passing off or unfair competition, registered designs, other rights in designs any application or right of application of such rights, including codes, sequences, derivative works, copyrights, data-base rights, trade secrets, know-how, business names, trade names, trademarks, service marks, patents, petty patents, utility models, rights in design, organization, structure, interfaces, any documentation, data and other related rights

Personal Data has the meaning given to it according to Regulation (EU) 2016/679 and Directive 95/46/EC, as amended from time to time

Processor has the meaning as defined by Regulation (EU) 2016/679 with obligations as set forth in the regulation

SCW means Secure Code Warrior Limited, and its related/ affiliate entities

SCW Learning Platform means computer software developed and owned by SCW Limited, a company incorporated in England, made available to the Customer as a service via the internet, including Documentation, updates, supplements, modification, addition and/or adaptation of the SCW Learning Platform to enable or include certain features and/or functionality, under the terms and conditions of this Agreement

SLAs means the Service Level Schedule located at https://securecodewarrior.com/service-level-agreement

Subscription means the subscription for the right to access and use the SCW Learning Platform according to this Subscription Agreement

Sub Processor means a 3rd party processor selected by SCW for a specific set of processing needed by the SCW Learning Platform

1.2. The headings of the Subscription Agreement are for convenience only and shall not constrain or affect its construction or interpretation in any way whatsoever. Words importing the singular shall include the plural, and vice versa. Sections, addendums and headings do not affect the interpretation of this Subscription Agreement.

2. SCW LEARNING PLATFORM

2.1. The SCW Learning Platform provides an integrated suite of secure code training and tools that moves the focus from reaction to prevention. SCW's Learning Platform includes hands-on training, tournaments, courses, self-paced learning for every skill level and online assessments.

2.2. The SCW Learning Platform is made available through an account set up for the Customer. The Customer's right to access and use the Subscription for the SCW Learning Platform is web based only pursuant to the terms of this Subscription Agreement.

3. TERM

3.1. This Subscription Agreement commences on the date, and for the period set out in the applicable order form unless terminated in accordance with this Subscription Agreement or renewed by agreement.

3.2. On termination or expiration of the Subscription Agreement, the Customer´s access to and use of the SCW Learning Platform will no longer be available, neither the Customer or the End User(s), will have access to or use of the SCW Learning Platform and applicable data or Documentation therein.

4. CUSTOMER RIGHTS AND RESTRICTIONS

4.1. The Customer (including its End Users) is granted a limited, non-transferable, non-exclusive subscription to access and use the SCW Learning Platform on Devices via any standard web browser during the Subscription Term.

4.2. Neither Customer nor any End User are permitted to frame, reproduce, or otherwise re-publish, re-sell or re-distribute the SCW Learning Platform, or any part thereof.

4.3. The Customer agrees, and will procure that it's End Users, will only access and use the SCW Learning Platform for its internal business use.

4.4. The Customer must not, and will procure that it's End Users do not:
(a) access or use the SCW Learning Platform in any way that causes or may cause damage to the SCW Learning Platform or impairment of the availability or accessibility of the SCW Learning Platform or any of the areas of or services on the SCW Learning Platform
(b) access or use the SCW Learning Platform in any way that is unlawful, illegal, fraudulent or harmful or in connection with any unlawful, illegal, fraudulent unethical, immoral, inappropriate or harmful activity, including but not limited to, to exploiting or acquiring skills for illegal or malicious attacks

(c) allow its End Users or any third party to attempt, to copy, modify, duplicate, create derivative works, mirror, republish, reverse compile, disassemble, reverse engineer, download, transmit, or distribute all or any portion of the SCW Learning Platform, including but not limited to the object code and the source code, in any form or media or by any means
(d) rent, lease, distribute, sell, sublicense, transfer or provide access to or use of the SCW Learning Platform to any third party; and
(e) access or use the SCW Learning Platform for any commercial purpose or for any public display, whether commercial or non-commercial, without the prior written approval of SCW.

4.5. The Customer acknowledges and agrees that the SCW Learning Platform may include certain software which is incorporated in the SCW Learning Platform for no additional fee (Open Source Software) Access to the Open Source software is provided subject to the terms provided for such access. A link to the relevant terms is https://license-list.secure.com. The Customer herein agrees that such terms are incorporated into this Subscription Agreement.

5. SUPPORT

5.1. Customer acknowledge and agree that SCW will maintain the SCW Learning Platform and provide all support services on terms set out in the SLAs, attached to this EULA as Attachment A.

6. FEES and PAYMENTS

6.1. The Subscription Fee including payment terms, number of End Users are set out in the applicable order form, and may be updated from time to time. For clarity, the Customer may add additional End Users, subject to agreement to pay an additional fee.

7. CONFIDENTIALITY

7.1. Each party agrees to protect Confidential Information disclosed to it to the same extent and in the same manner that it would protect its own Confidential Information. Each party further agrees to bind their respective employees, agents and subcontractors to the confidentiality and other terms and conditions of the Agreement and to be liable for their compliance therewith. In no event shall either parties' practices and/ or policies fall below a level of reasonable and due care, which includes each party limiting reproduction, access, disclosure and use to those personnel who have a need to know for the purposes of performing the services in this Agreement, and who are made aware of and agree to comply with the terms of the confidentiality obligations herein. SCW recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor.

8. INTELLECTUAL PROPERTY

8.1. SCW owns and retains all right, title, interest and ownership to the SCW Learning Platform including without any limitation all Intellectual Property rights in and to the SCW Learning Platform, Documentation, and learning materials. Accordingly, the Customer acknowledges and agrees that this Subscription Agreement and its access and use of the SCW Learning Platform transfers no title or ownership of the SCW Learning Platform either to it or any of its End Users.

8.2. The Customer acknowledges and agrees that SCW has a royalty-free, worldwide, transferable, irrevocable, perpetual license to use or incorporate into the SCW Learning Platform any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including End Users, relating to the operation of the SCW Learning Platform.

9. WARRANTIES

9.1. The Customer acknowledges and agrees that:

(a) SCW makes no representation regarding the SCW Learning Platform other than as stated in this Subscription Agreement;

(b) it has relied on its own skill and judgment or that of its advisers in entering to enter into this Subscription Agreement; and

(c) the SCW Learning Platform including all Documentation comprise a standard service and materials provided to SCW's customers generally and they have not been developed to meet the Customer's or any of the Affiliates requirements.

10. SUSPENSION

10.1. SCW reserves the right to temporarily suspend the Customers access to and use of the SCW Learning Platform in circumstances set out in clause 12.2(b) below and if any of the following occur or SCW has reasonable grounds to suspect:

(a) there has or may have been, a breach of security (including the introduction of any Malicious Code), a breach of this Subscription Agreement, or any unlawful or illegal use of the Service and the Documentation;

(b) SCW knows or has reasonable grounds to suspect that any of the Customer Data infringes the Intellectual Property Rights or other rights of any third party, or is in any way unlawful, or is likely to lead to any third party instituting or threatening legal proceedings against SCW or any other person;

(c) the Customer or any of the Affiliates cause, the Customer, its End Users, and/ or other employees including those of any of its Affiliates has caused any technical or

security issue which affects the Service or other customers of SCW or of any SCW Affiliate; and/ or
(d) in circumstances set out in clause 12.2 below.

11. INSURANCE

11.1. Each party agrees, during the Subscription Term, to maintain appropriate insurances as required by applicable law and which include all insurances as required by applicable laws and regulations and employers' liability insurance, Public and Product liability and Professional Indemnity.

12. TERMINATION

12.1. Either party may terminate the Subscription Agreement and any applicable Subscription Order by notice in writing to the other and with immediate effect if any law enforcement agency or court requires or requests SCW to do so

12.2. SCW may temporarily suspend the Subscription Agreement at any time in circumstances where there are technical and or security issues caused by the Customer that directly impact (or may impact) either of (a) the business operations of SCW or any of its customers; (b) the integrity of the SCW Learning Platform. For clarity, SCW will provide the Customer with a period of 14 days to respond to and or resolve any issues or concerns that Secure Code Warrior identifies in writing to the Customer, but the decision will otherwise be exercised by Secure Code Warrior in its absolute discussion.

13. LIMITATION OF LIABILITY

13.1. The maximum liability of SCW to the Customer will in no circumstances exceed an amount equal to or more than the Subscription Fee paid or payable to SCW for access to and use of the SCW Learning Platform, in any 12 month period.

13.2. Notwithstanding the above, neither Party will be liable to the other, whether in contract or tort, or otherwise for any incidental, indirect, punitive, exemplary, special, consequential or unforeseeable loss, damage or expense, loss of profits, loss of business, loss of opportunity, loss or corruption of data, however arising, even if advised of the possibility of such loss or damages being incurred.

13.3. NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS SECTION SHALL BE DEEMED TO IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF, OR RELATED TO, THIS AGREEMENT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31. U.S.C. §§ 3729-3733.

14. GOVERNING LAW

14.1. This agreement is subject to the Contracts Disputes Act of 1978 (41. U.S.C §§ 7101-7109) and Federal Tort Claims Act (28 U.S.C. §1346(b)). The validity, interpretation and enforcement of agreement will be governed by and construed in accordance with the federal laws of the United States.

15. MISCELLANEOUS

15.1. This Subscription Agreement and the Customer's right to access and use the SCW Learning Platform does not establish any relationship of partnership, joint venture, employment, franchise or agency between the Customer and SCW.

15.2. Survival. Sections of this Subscription Agreement that, by their terms, require performance after the termination or expiration of this Subscription Agreement will survive as permitted by local law. These sections include section 1 (Definition), section 7 (Confidentiality), section 8 (Intellectual property), section 9 (Warranties), and section 14 (Miscellaneous).

15.3. Entire agreement. This Subscription Agreement (including the Service Level Schedule), and where relevant, any Data Processing Agreement constitutes the entire agreement between SCW and the Customer. It supersedes any prior or contemporaneous communications, and any prior agreement between the Parties regarding its subject matter, and cannot be amended or updated other than by a written agreement signed by both Parties. In the event of a conflict between the terms of this Subscription Agreement and a subsequent written agreement, this Subscription Agreement shall prevail.

15.4. Waiver. No waiver of any breach of this Subscription Agreement shall be a waiver of any other breach, and no waiver will be effective unless made in writing and signed by an authorized representative of the waiving Party.

15.5. Severability. If a court holds any provision of this Subscription Agreement to be illegal, invalid or unenforceable, the remaining provisions will remain in full force and effect and the Parties will amend this Subscription Agreement to give effect to the stricken section to the maximum extent possible.

ATTACHMENT A - SERVICE LEVEL AGREEMENT

1) DEFINITIONS

Agreement means the agreement between the parties to which this schedule is appended
Customer includes its subsidiaries/ affiliates entities

Customer Help Desk means the internal support desk established by the Customer qualified to support the Services within the Customer's operations

Business Day means a Day on which the Customer is open for business at a office location using the Service

Day means a calendar day

Maintenance and Support Services means the maintenance and support services to be provided by SCW as described in this Schedule

Minimum Service Level means the minimum Service Levels to be achieved by SCW as set out in this Schedule

Response Times means the time period commencing with notification from the Customer of an incident and ends with the initial response from SCW

Resolution Time means the time period commencing with notification being received from the Customer and ending with a response or deemed response from the Customer Help Desk that an item has been resolved

Service means the online security learning service to be provided by SCW to the Customer

Service Credits means the applicable service credits as described in 2(f) of the Service Levels

Service Hours means, in respect of each week of the Term, the period from the start of the first business day in the first location from which Customer accesses the Services to the end of the last Business day in the relevant week in the last location from which Customer accesses the Services

Service Levels means the performance levels to which the Services shall be provided as set out in this Schedule

Service Period means each calendar month that Customer receives the Services

Service Up Time Percentage means the total number of minutes in a calendar month minus the number of minutes of downtime suffered in a calendar month, divided by the total number of minutes in a calendar month minus scheduled downtime

System Response Time means the time required for the Service to respond to an input as set

Term means the term for which the Customer has subscribed to the Service

Up Time has the meaning set out in 2(e)(iii) of the Service Levels

2) SERVICES SPECIFICATION

a) GENERAL

i) This schedule describes the scope and functionality of the Services to be provided by SCW to the Customer under this Subscription Agreement. It also specifies certain of the obligations of each party in the delivery of the Services.

ii) Each Service has, where specified, an associated Service Level

b) SERVICES

i) SCW shall supply Customer with an online security learning service incorporating the following production environment services

(a) Online Access: On-line access to the Service during the Service Hours excluding scheduled downtime as defined in this schedule or as otherwise agreed in writing between the parties

(b) Maintenance and Support Services during the Service Hours

(c) Data back-ups in accordance with section 5

(d) Application management:

(a) application upgrades,

(b) delivery of application maintenance updates

ii) SCW shall monitor and manage all components used to deliver the Service during the Service Hours throughout the Term

iii) SCW shall ensure appropriate capacity planning of the Services to ensure there is always sufficient capacity to provide the Service at the Service Levels. This shall require Customer to advise SCW of any anticipated material changes to the use of the Service

c) REPORTING

i) SCW shall make available to authorized Support Contacts a monthly management report detailing the performance of the Service against the Service Levels

3) MAINTENANCE AND SUPPORT SERVICES

a) RELEASE STRATEGY

i) SCW will inform Customer regularly of the timing and contents of new releases to the Service. Customer may provide suggestions and input to SCW regarding any planned or requested new features. SCW shall, at its sole discretion, consider whether Customer's suggestions shall be included in a subsequent release as part of the Maintenance and Support Services

ii) Except where a product enhancement cost has been agreed with the Customer, such new releases to the Service shall be made at no cost to the Customer

iii) SCW shall document any such changes in release notes which shall be made available to the Customer as soon as possible, but no later than the date any new release is issued.

b) SUPPORT SERVICES & RESPONSIBILITIES

i) SCW shall provide the support services in English

ii)SCW shall notify Customer of all incidents that may have an impact on the Service provided to the Customer

iii) SCW shall be responsible for:

(a) The availability of the Service

(b) Solving incidents and problems raised by the Customer Help Desk

(c) Implementing changes to the Service required as a result of solving incidents

(d) Communicating the status of incidents to the Customer Help Desk

(e) Communicating information about planned system changes of outages to Customer and the subsidiaries in a timely manner

(f) Responding to each incident in line with the specified actions for each incident class

iv) Customer is responsible for:

(a) Raising incidents to the SCW help desk through a centralized Customer Help Desk

(b) The Customer must nominate at least 2 and not more than [X] authorized Support Contacts and notify SCW of their names and contact details immediately following the date of the Agreement.

(c) Incidents and service requests must be reported by email by an authorized Support Contact to support@securecodewarrior.com

(d) No phone support is provided directly to Users

(e) The Customer must not publish SCW's contact details on their intranet, website or anywhere else.

c) INCIDENT MANAGEMENT

i) The Customer Help Desk shall provide the following items when notifying SCW of an incident

(a) Incident time, duration and location

(b) User ID and contact details

(c) Incident description

(d) Category of incident, to be mutually agreed between the parties.

d) INCIDENT CATEGORIZATION

i) Class A – Severe Impact Provision of Service Failure

(a) An incident that results in the loss of all or a significant portion of the service and impacts a majority of the users.

ii) Class B – Major Impact Provision of Service Failure

(a) The service is accessible by means of a workaround, or only a small number of users are impacted Or an incident which materially affects the performance of the Services in a negative manner or materially restricts the Customer's use of the Service

iii) Class C – Moderate Impact

(a) Incidents occur which do not individually represent a failure of the service, but are agreed as defects Or an incident which only has a minor effect on the Customer's use of the Service or an Incident which is not a Class A or B incident

iv) Class D – Low Impact

(a) A general question or concern raised by the Customer concerning the use or implementation of the Service

e) RESPONSE TIMES

i) The SCW help desk will acknowledge receipt of the incident report within no more than one hour.

f) RESOLUTION TIME

i) In the event of a Class A incident SCW will immediately assign necessary staff to work on the incident until resolved or a workaround is provided to the Customer.

ii) For Class B and C incidents SCW and the Customer will agree an acceptable timeframe within which the incident should be resolved, such agreement to occur within:

(a) 2 working days for a Class B incident; and

(b) 10 working days for a Class C incident.

iii) For Class D incidents within such period of time as SCW deems appropriate given the nature of the question or concern

g) CLOSURE OF INCIDENTS

i) Before closing an incident, the SCW help desk will seek confirmation of the Customer that the incident has been resolved.

4) SERVICE LEVELS

a) GENERAL DESCRIPTION OF SERVICE LEVELS

i) Unless otherwise specified, the measurement period for the Service Levels is each Service Period.

ii) Where Service Levels are described as "targeted", such targeted Service Level measurements represent the expected performance levels of the Service under normal operating conditions, but such targeted measurements are for guidance only and do not constitute any obligations or liabilities on the part of SCW and any failure to meet such targeted Service Levels shall not be construed in any way as a breach by SCW of this Agreement.

iii) In the event that Service Levels fail to meet the targeted Up Time and/or the targeted System Response Time metrics in any Service Period, SCW's obligations are limited to providing an analysis and explanation of the reason(s) and proposed reasonable measures to eliminate the undershoot. Such measures may require changes either in the usage of the Services by the Customer, or of the Services by SCW.
iv) Where Service Levels are described as 'contracted', such contracted Service Level measurements represent the actual performance levels of the Service under normal operating conditions, and a failure to meet such contracted Service Levels will result in Service Credits being calculated.

b) UPTIME AND PERFORMANCE SERVICE LEVELS

i) The Service Levels apply to the SCW learning platform and shall be measured over the Service Hours except for scheduled maintenance periods.
ii) The metrics used to measure performance of the Service are as follows:
(a) System Response Time
(b) Up Time
(c) Maintenance Window
iii) The point of measurement for all Services monitoring with respect to System Response time shall be the servers at the SCW sub-processor data center. Response times exclude the transaction cycle times on communication links from the data center to the Customer's end user.
iv) System Response Time % of Service Period that Response Times will be met
(a) Targeted 5 seconds 90%
(b) Contracted 10 seconds 99%
(c) Contracted 15 seconds 99.75%
v) The System Response metric shall be calculated over a Service Period
vi) Measurement methods and targets for Service Up Times shall be as follows:
(a) Service Up Time shall be calculated at the end of each Service Period. The contracted Service level for Service Up Times in any service period shall be 99.75%. The targeted Service Level for Services Up Times in any Services Period shall be 99%.
(b) Up Time shall be expressed in percent and is defined as the time period during which the Service is available to the customer
(c) Up Time is calculated as follows:
(a) Service Up Time in % = means total number of minutes in the calendar month minus scheduled downtime minus the number of minutes of downtime suffered in a calendar month, divided by the total number of minutes in a calendar month minus scheduled maintenance windows
vii) Service Credits shall apply for failure to meet the contracted Service Levels and shall be as follows

(a) For Uptime Percentage less than 99.75% but equal to or greater than 99.0%, you will be eligible for a 10% Service Credit of the Service fee for the applicable month.
(b) For Uptime Percentage less than 99.0%, you will be eligible for a 20% Service Credit.
(c) The Service Fee shall be the total service fee paid divided by the number of months of subscription to the service during a Term
(d) SCW shall provide the Service Credit to the Customer in the month following the Service Period in which the Service Level Failure occurred

c) MAINTENANCE WINDOWS

i) The provisions for scheduled maintenance are as follows:

(a) Frequency: Weekly
(b) Duration: Maximum of two (2) hours)
(c) Time Monday 11am-1pm Sydney time (AEST/ADST)

ii) Unplanned maintenance including corrective actions to be taken by SCW to resolve an incident

d) SERVICE LEVEL EXCLUSIONS

i) The parties agree that the Service Levels shall not apply if one or more of the following exists:

(a) Suspension of the Service to carry out planned or routine maintenance
(b) Adverse impact on Up Times or Response Times due to the malfunction of Customer owned or controlled firewalls, networks or connectivity.
(c) Adverse impact on Up Times or Response Times due to a Force Majeure event(s)

e) BACK-UPS

i) SCW shall take a backup of all Customer data:

(a) Incremental Backup: Every Minute, retained for 24 hours
(b) Full backup: Every 6 hours, retained for 2 calendar days
(c) Full backup: Every day retained for 7 calendar days
(d) Full backup: Every week retained for 4 calendar weeks
(e) Full backup: Every month retained for 13 months

ii) Such backup shall be stored at a separate, secure, location to the production environment

iii) Backup data shall only be used for resolving an incident reported by the Customer