Federal Supply Service
Authorized Federal Supply Schedule Price List
On-line 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-driven database system. The INTERNET address GSA Advantage! ® is: GSAAdvantage.gov.

SPECIAL ITEM NUMBER 54151S INFORMATION TECHNOLOGY PROFESSIONAL SERVICES
SPECIAL ITEM NUMBER 54151HACS HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
SPECIAL ITEM NUMBER 54151 SOFTWARE MAINTENANCE SERVICES
SPECIAL ITEM NUMBER 511210 SOFTWARE LICENSES
SPECIAL ITEM NUMBER OLM – ORDER-LEVEL MATERIALS (OLMs)

Redport Information Assurance, LLC
814 W Diamond Avenue. Ste. 370
Gaithersburg, MD 20878
Office: 703-229-6709
Fax: 703-229-6708

Contract Number: **47QTCA18D001N**

Period Covered by Contract: **October 31, 2017 through October 30, 2022**

General Services Administration
Federal Acquisition Service

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.
Contract period

MULTIPLE AWARD SCHEDULE (MAS)

Customer Information:

1a. Table of Awarded Special Item Number(s) with appropriate cross-reference to page numbers:

SIN	Description
54151S	IT Professional Services
54151	Software Maintence Services
511210	Software Licenses
54151HACS	Highly Adaptive Cybersecurity Services
OLM	Order-Level Materials (OLMs)

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. See page 30

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. Starting on Page 14

2. Maximum Order: $500,000.00

3. Minimum Order: $100.00

4. Geographic Coverage (delivery Area): Domestic (48 States, DC) 54151 for SIN 54151S and 54151HACS only. Worldwide coverage for 54151 and 511210

5. Point(s) of production (city, county, and state or foreign country): IL for 511210

6. Discount from list prices or statement of net price: Government net prices (discounts already deducted).

7. Quantity discounts: 1% on Sales over $250,000 for SIN 54151S and 54151HACS only

8. Prompt payment terms: Net 30 days

9a. Notification that Government purchase cards are accepted up to the micro-purchase threshold: Yes

9b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold: will not accept over the micropurchase threshold

10. Foreign items (list items by country of origin): 511210 IL

11a. Time of Delivery (Contractor insert number of days): Specified on the Task Order and shall deliver or perform services in accordance with the terms negotiated in an agency's order.

11b. 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 list that have expedited delivery: Contact Contractor

11c. 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: Contact Contractor

11d. 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 effect a faster delivery: Contact Contractor

12. F.O.B Points(s): Destination

13a. Ordering Address(es):

Redport Information Assurance, LLC
814 W Diamond Avenue. Ste. 370
Gaithersburg, MD 20878

13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's), and a sample BPA can be found at the GSA/FSS Schedule homepage (fss.gsa.gov/schedules).

14. Payment address(es):

Redport Information Assurance, LLC
814 W Diamond Avenue. Ste. 370
Gaithersburg, MD 20878

15. Warranty provision.: Contractor's standard commercial warranty.

16. Export Packing Charges (if applicable): N/A

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level): Contact Contractor

18. Terms and conditions of rental, maintenance, and repair (if applicable): N/A

19. Terms and conditions of installation (if applicable): N/A

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): N/A

20a. Terms and conditions for any other services (if applicable): N/A

21. List of service and distribution points (if applicable): N/A

22. **List of participating dealers (if applicable):** N/A

23. **Preventive maintenance (if applicable):** N/A

24a. **Environmental attributes, e.g., recycled content, energy efficiency, and/or reduced pollutants:** N/A

24b. **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. contactor's website or other location.) The EIT standards can be found at:** www.Section508.gov/.

25. **Data Universal Numbering System (DUNS) number:** 966193638

26. **Notification regarding registration in the System for Award Management (SAM) Database:** Registered

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

NOTE: The Transactional Data Reporting (TDR) Rule requires vendors to electronically report the price the federal government paid for an item or service purchased through GSA acquisition vehicles. The TDR PILOT DOES NOT APPLY TO THIS SIN, EXCEPT if a TDR-covered SIN(s) is proposed as part of your total offering to GSA (If both TDR and NON TDR SINs are offered, then the entire contract is subject to TDR and the Price Reduction Clause (PRC) and Commercial Sales Practice (CSP) requirements are removed for the entire contract." If NON TDR SIN(s) are offered only, then the offering will be subject to the PRC and CSP

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must 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-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M -07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- 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 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- 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 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

****NOTE: All non-professional labor categories must be incidental to, and used solely to support Highly Adaptive Cybersecurity Services, and cannot be purchased separately.

****NOTE: All labor categories under the Special Item Number 132-51 Information Technology Professional Services may remain under SIN 132-51 unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.

1. SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132- 45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132¬33, 132-8), and may be quoted along with services to provide a total solution.

c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.

d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

e. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. ORDER

a. Agencies may use written orders, Electronic Data Interchange (EDI) orders, Blanket Purchase Agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

3. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015) (TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (MAY 2014) Rights in Data – General, may apply.

The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to the ordering activity's security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

7. INDEPENDENT CONTRACTOR

All Highly Adaptive Cybersecurity Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

"Contractor" means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party

to this contract.

"Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b) To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the

ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives,

directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

10. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting

Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates,, minimum general experience

minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004)

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities

- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelors of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

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

1. SCOPE

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. **ORDER**

a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. **PERFORMANCE OF SERVICES**

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. **STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)**

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

(b) If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES

The Inspection of Services–Fixed Price (AUG 1996) (Deviation – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (MAY 2001) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

7. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. INDEPENDENT CONTRACTOR

All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

"Contractor and its affiliates" and "Contractor or its affiliates" refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

11. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for IT Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—

(1) The offeror;

(2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS

Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 132-51 IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all IT Professional Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented:

EXAMPLE: Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, structure and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, conducts feasibility studies.

Minimum Education: Bachelor’s Degree in Computer Science

LABOR CATEGORY DESCRIPTIONS (54151S)

Labor Category	Functional Responsibility	Education	Years Experience
C&A/A&A Analyst	Provides support in all facets of the C&A process relative to both classified and unclassified networks in in a fast paced, dynamic environment. Has comprehensive knowledge of information security principles as it applies to military networks, standards, and systems. Serve as Information Assurance point of contact for promotional, test, new, replacement and/or Contractor equipment being brought into the purview of the accreditation boundary. Ensure the system/program managers provide proper accreditation documentation and make necessary changes/additions to the DIACAP packages. Prepare and maintain DIACAP artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy IA controls).	Associates	2

C&A/A&A Engineer	Provides support in all facets of the C&A process relative to both classified and unclassified networks in in a fast paced, dynamic environment. Has comprehensive knowledge of information security principles as it applies to military networks, standards, and systems. Serve as Information Assurance point of contact for promotional, test, new, replacement and/or Contractor equipment being brought into the purview of the accreditation boundary. Ensure the system/program managers provide proper accreditation documentation and make necessary changes/additions to the DIACAP packages. Prepare and maintain DIACAP artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy IA controls).	Bachelors	4
Digital Forensics Engineer	Preserves, harvests, and processes electronic data according to policies and practices. Performs forensic analysis and has an understanding and interest in performing digital forensics in a cloud environment. Provides creative and innovative solutions for client matters. Forms and articulates expert opinions based on analysis and drafts export reports, affidavits, and other expert testimony.	Bachelors	4

Penetration Tester	Conducts formal tests on web-based applications, networks, and other types of computer systems on a regular basis. Expected to work on physical security assessments of servers, computer systems, and networks. Conducting regular security audits from both a logical/theoretical standpoint and a technical/hands-on standpoint. Expected to work on the security of wireless networks, databases, software development, and/or company secrets.	Bachelors	6
Security SME	Performs assessment of present levels of cyber security, defines acceptable levels of risk, trains all personnel in proper cyber hygiene and establishes formal maintenance procedures. Performs privacy impact assessments and provides PII data security and monitoring, and migration strategies. Identifies potential vulnerabilities to cyber and information security using penetration testing and red teams. Provides technologies for identification, modeling, and predictive analysis of cyber threats.	Bachelors	8
Technical Writer	Assists in collecting and organizing information required for preparation of user's manuals, training materials, installation guides, proposals, and reports. Edits functional descriptions, system specifications, user's manuals, special reports, or any other customer deliverables and documents.	Associates	2

Cyber Security Engineer II	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.	Bachelors	4
Information Assurance Specialist	Provides technical support in the areas of vulnerability assessment, risk assessment, network security, product evaluation, and security implementation. Analyzes the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Responsible for designing and implementing solutions for protecting the confidentiality, integrity and availability of sensitive information. Ensures that all information systems are functional and secure. Provides technical evaluations of customer systems and assists with making security improvements. Participates in design of	Bachelors	6

	information system contingency plans that maintain appropriate levels of protection and meet time requirements for minimizing operations impact to customer organization. Conducts security product evaluations, and recommends products, technologies and upgrades to improve the customer’s security posture. Conducts testing and audit log reviews to evaluate the effectiveness of current security measures.		
Cyber Security/Information Assurance Auditor	Provides an audit of security systems used. Provides a detailed report of information systems that outline whether the system runs efficiently or effectively. Tests policies to determine whether there are risks associated with them. Reviews or interviews members of the staff to learn about any security risks or other complications within the company.	Bachelors	6
Cyber Security Engineer III	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of	Bachelors	6

	computer systems and applications during all phases of the system development life cycle.		
Security Software Engineer Team Lead	Performs design, programming, documentation, and implementation of applications that require knowledge of information systems and related systems concepts for effective development and deployment of software modules. Participates in all phases of software development with emphasis on the design, coding, testing, documentation, and acceptance phases. Designs and prepares technical reports and related documentation. Perform as the primary software engineering expert on a major automated information system development project. Analyze and study complex system requirements. Design software tools and subsystems to support and manage their implementation. Manage software development and support using formal specifications, data flow diagrams, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedules. Review existing programs and assist in making refinements, reducing operating time, and improving current development methods. Establish and manage software configuration.	Bachelors	6

Incident Response Lead	Familiar with industry standard malware reverse analysis methodologies. Possess knowledge of various malware encryption and compression / packing methodologies and protective encryption weaknesses. Ability to provide malware threat research on new attacks and exploits. Ability to script (ex. Python and/or PERL) and automate tasks and be able to discern malware based covert channel and command and control protocol analysis. Apply the proper techniques and procedures to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.	Bachelors	6
Network Security Engineer III	Responsible for the implementation, maintenance, and integration of WAN, LAN, and server architecture. Responsible for implementation and administration of network security hardware and software, enforcing the network security policy and complying with requirements of external security audits and recommendations. Performs analysis of network security needs and contributes to design, integration, and installation of hardware and software. Analyzes, troubleshoots and corrects network problems remotely and on-site. Maintains and administers perimeter security systems such as firewalls and intrusion detection systems.	Bachelors	6

Cyber Security Program/Project Manager	Manages more than one functional area in information systems design, development, and analysis encompassing one or more of the following areas of technical expertise: programming, computer application analysis, software development, systems integration, and related disciplines. Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments, salary, and recognition/disciplinary actions.	Bachelors	8
Security Administrator	Teaches others about computer security, checks for security violations, installs protection software and takes action against cyber attacks. Provides evidence of a cyber attack to prosecute individuals for breaching security. Must have excellent communication skills, as well the ability to detect and analyze problems. Expected to quickly and accurately find a solution.	Associates	2
Cyber Security Engineer I	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network	Associates	2

	security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.		

LABOR CATEGORY DESCRIPTIONS (54151HACS)

Labor Category	Functional Responsibility	Education	Years Experience
C&A/A&A Analyst	Provides support in all facets of the C&A process relative to both classified and unclassified networks in in a fast paced, dynamic environment. Has comprehensive knowledge of information security principles as it applies to military networks, standards, and systems. Serve as Information Assurance point of contact for promotional, test, new, replacement and/or Contractor equipment being brought into the purview of the accreditation boundary. Ensure the system/program managers provide proper accreditation documentation and make necessary changes/additions to the DIACAP packages. Prepare and maintain DIACAP artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy IA controls).	Associates	2

C&A/A&A Engineer	Provides support in all facets of the C&A process relative to both classified and unclassified networks in in a fast paced, dynamic environment. Has comprehensive knowledge of information security principles as it applies to military networks, standards, and systems. Serve as Information Assurance point of contact for promotional, test, new, replacement and/or Contractor equipment being brought into the purview of the accreditation boundary. Ensure the system/program managers provide proper accreditation documentation and make necessary changes/additions to the DIACAP packages. Prepare and maintain DIACAP artifacts/packages (e.g. Configuration Management Plan, Vulnerability Management Plan, System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy IA controls).	Bachelors	4
Digital Forensics Engineer	Preserves, harvests, and processes electronic data according to policies and practices. Performs forensic analysis and has an understanding and interest in performing digital forensics in a cloud environment. Provides creative and innovative solutions for client matters. Forms and articulates expert opinions based on analysis and drafts export reports, affidavits, and other expert testimony.	Bachelors	4

Penetration Tester	Conducts formal tests on web-based applications, networks, and other types of computer systems on a regular basis. Expected to work on physical security assessments of servers, computer systems, and networks. Conducting regular security audits from both a logical/theoretical standpoint and a technical/hands-on standpoint. Expected to work on the security of wireless networks, databases, software development, and/or company secrets.	Bachelors	6
Security SME	Performs assessment of present levels of cyber security, defines acceptable levels of risk, trains all personnel in proper cyber hygiene and establishes formal maintenance procedures. Performs privacy impact assessments and provides PII data security and monitoring, and migration strategies. Identifies potential vulnerabilities to cyber and information security using penetration testing and red teams. Provides technologies for identification, modeling, and predictive analysis of cyber threats.	Bachelors	8
Cyber Security Engineer II	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical	Bachelors	4

	support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.		
Information Assurance Specialist	Provides technical support in the areas of vulnerability assessment, risk assessment, network security, product evaluation, and security implementation. Analyzes the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Responsible for designing and implementing solutions for protecting the confidentiality, integrity and availability of sensitive information. Ensures that all information systems are functional and secure. Provides technical evaluations of customer systems and assists with making security improvements. Participates in design of information system contingency plans that maintain appropriate levels of protection and meet time requirements for minimizing operations impact to customer organization. Conducts security product evaluations, and recommends products, technologies and upgrades to improve the customer's security posture. Conducts testing and audit log reviews to evaluate the effectiveness of current security measures.	Bachelors	6

Cyber Security/Information Assurance Auditor	Provides an audit of security systems used. Provides a detailed report of information systems that outline whether the system runs efficiently or effectively. Tests policies to determine whether there are risks associated with them. Reviews or interviews members of the staff to learn about any security risks or other complications within the company.	Bachelors	6
Cyber Security Engineer III	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.	Bachelors	6

Security Software Engineer Team Lead	Performs design, programming, documentation, and implementation of applications that require knowledge of information systems and related systems concepts for effective development and deployment of software modules. Participates in all phases of software development with emphasis on the design, coding, testing, documentation, and acceptance phases. Designs and prepares technical reports and related documentation. Perform as the primary software engineering expert on a major automated information system development project. Analyze and study complex system requirements. Design software tools and subsystems to support and manage their implementation. Manage software development and support using formal specifications, data flow diagrams, other accepted design techniques and Computer Aided Software Engineering (CASE) tools. Estimate software development costs and schedules. Review existing programs and assist in making refinements, reducing operating time, and improving current development methods. Establish and manage software configuration.	Bachelors	6
Incident Response Lead	Familiar with industry standard malware reverse analysis methodologies. Possess knowledge of various malware encryption and compression / packing methodologies and protective encryption weaknesses. Ability to provide malware threat research on new attacks and exploits. Ability to	Bachelors	6

	script (ex. Python and/or PERL) and automate tasks and be able to discern malware based covert channel and command and control protocol analysis. Apply the proper techniques and procedures to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.		
Network Security Engineer III	Responsible for the implementation, maintenance, and integration of WAN, LAN, and server architecture. Responsible for implementation and administration of network security hardware and software, enforcing the network security policy and complying with requirements of external security audits and recommendations. Performs analysis of network security needs and contributes to design, integration, and installation of hardware and software. Analyzes, troubleshoots and corrects network problems remotely and on-site. Maintains and administers perimeter security systems such as firewalls and intrusion detection systems.	Bachelors	6
Cyber Security Program/Project Manager	Manages more than one functional area in information systems design, development, and analysis encompassing one or more of the following areas of technical expertise: programming, computer application analysis, software development, systems integration, and related disciplines. Responsible for coordinating subordinate employee recruitment, selection and training, performance assessment, work assignments,	Bachelors	8

	salary, and recognition/disciplinary actions.		
Security Administrator	Teaches others about computer security, checks for security violations, installs protection software and takes action against cyber attacks. Provides evidence of a cyber attack to prosecute individuals for breaching security. Must have excellent communication skills, as well the ability to detect and analyze problems. Expected to quickly and accurately find a solution.	Associates	2
Cyber Security Engineer I	Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware and applications software. Detects, diagnoses, and reports related problems on both server and desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.	Associates	2

LABOR CATEGORY RATES (SEE SINS BELOW)- GSA SCHEDULE CONTRACT INFORMATION TECHNOLOGY (IT) SERVICES (All rates below incude IFF)

SIN	LCAT	10/31/2017-10/30/2018	10/31/2018-10/30/2019	10/31/2019-10/30/2020	10/31/2020-10/30/2021	10/31/2021-10/30/2022
54151S 54151HACS	*C&A/A&A Analyst*	$90.49	$ 92.30	$ 94.15	$ 96.03	$ 97.95
54151S 54151HACS	*C&A/A&A Engineer*	$102.12	$ 104.16	$ 106.25	$ 108.37	$ 110.54
54151S 54151HACS	*Digital Foresnsics Engineer*	$146.17	$ 149.09	$ 152.08	$ 155.12	$ 158.22
54151S 54151HACS	*Penetration Tester*	$128.54	$ 131.11	$ 133.73	$ 136.41	$ 139.14
54151S 54151HACS	*Security SME*	$189.71	$ 193.50	$ 197.37	$ 201.32	$ 205.35
54151S	*Technical Writer*	$62.61	$ 63.86	$ 65.14	$ 66.44	$ 67.77
54151S 54151HACS	*Cyber Security Engineer II*	$113.78	$ 116.06	$ 118.38	$ 120.74	$ 123.16
54151S 54151HACS	*Information Assurance Specialist*	$169.02	$ 172.40	$ 175.85	$ 179.37	$ 182.95

54151S *54151HACS*	*Cyber Security/Information Assurance Auditor*	$131.58	$ 134.21	$ 136.90	$ 139.63	$ 142.43
54151S *54151HACS*	*Cyber Security Engineer III*	$152.95	$ 156.01	$ 159.13	$ 162.31	$ 165.56
54151S *54151HACS*	*Security Software Engineer Team Lead*	$165.16	$ 168.46	$ 171.83	$ 175.27	$ 178.77
54151S *54151HACS*	*Incident Response Lead*	$141.53	$ 144.36	$ 147.25	$ 150.19	$ 153.20
54151S *54151HACS*	*Network Security Engineer III*	$152.95	$ 156.01	$ 159.13	$ 162.31	$ 165.56
54151S *54151HACS*	*Cyber Security Program/Project Manager*	$171.61	$ 175.04	$ 178.54	$ 182.11	$ 185.76
54151S *54151HACS*	*Security Administrator*	$69.29	$ 70.68	$ 72.09	$ 73.53	$ 75.00
54151S *54151HACS*	*Cyber Security Engineer I*	$90.47	$ 92.28	$ 94.12	$ 96.01	$ 97.93

SIN 511210 Software Licenses and 54151 Software Maintenance Services

SIN	MANUFACTURER NAME	MFR PART NO	PRODUCT NAME	PRODUCT DESCRIPTION	GSA Rate Including IFF
511210	SAFE-T	ZZPMU-AN-49	ZoneZero SDP MSSP Model	Safe-T user. Price for 25-49 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 106.00
511210	SAFE-T	ZZPMU-AN-100	ZoneZero SDP MSSP Model	Safe-T user. Price for 50-100 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 99.20
511210	SAFE-T	ZZPMU-AN-250	ZoneZero SDP MSSP Model	Safe-T user. Price for 101-250 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 90.44
511210	SAFE-T	ZZPMU-AN-500	ZoneZero SDP MSSP Model	Safe-T user. Price for 251-500 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 84.61
511210	SAFE-T	ZZPMU-AN-1,000	ZoneZero SDP MSSP Model	Safe-T user. Price for 501-1,000 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 76.83
511210	SAFE-T	ZZPMU-AN-2,500	ZoneZero SDP MSSP Model	Safe-T user. Price for 1,001-2,500 users. (includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 69.05
511210	SAFE-T	ZZPMU-AN-5,000	ZoneZero SDP MSSP Model	Safe-T user. Price for 2,501-5,000 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 60.29
511210	SAFE-T	ZZPMU-AN-10,000	ZoneZero SDP MSSP Model	Safe-T user. Price for 5,001-10,000 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 49.60
511210	SAFE-T	ZZPMU-AN-20,000	ZoneZero SDP MSSP Model	Safe-T user. Price for 10,000-20.000 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 34.03
511210	SAFE-T	ZZPMU-AN-30,000	ZoneZero SDP MSSP Model	Safe-T user. Price for 20,000-30.000 users. (Includes User & VM Server Licenses) Supporting up to 5,000 concurrent connection	$ 23.34

511210	SAFE-T	ZZPU-AN-49	ZoneZero SDP - Annual SMB Price on Premises	Safe-T user. Price for 25-49 users (Includes User & Server Licenses) Supporting up to 500 concurrent connection	$ 101.14
511210	SAFE-T	ZZPU-AN-100	ZoneZero SDP - Annual SMB Price on Premises	Safe-T user. Price for 50-100 users. (includes User & Server Licenses) Supporting up to 500 concurrent connection	$ 97.26
511210	SAFE-T	ZZPU-AN-250	ZoneZero SDP - Annual SMB Price on Premises	Safe-T user. Price for 101-250 users. (includes User & Server Licenses) Supporting up to 500 concurrent connection	$ 89.47
511210	SAFE-T	ZZPU-AN-500	ZoneZero SDP - Annual SMB Price on Premises	Safe-T user. Price for 251-500 users. (includes User & Server Licenses) Supporting up to 500 concurrent connection	$ 79.74
511210	SAFE-T	ZZ_SDP-PAN-AC	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T Access Controller virtual appliance. Supporting up to 5,000 concurrent connection	$ 3,890.04
511210	SAFE-T	ZZ_SDP-PAN-AGW	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T Access Gateway virtual appliance. Supporting up to 5,000 concurrent connection	$ 1,458.77
511210	SAFE-T	ZZ_SDP-PAN-AUTHGW	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T Authentication Gateway virtual appliance. Supporting up to 5,000 concurrent connection	$ 1,458.77
511210	SAFE-T	ZZPU-AN-1,000	ZoneZero SDP - Annual Enterprise Price on	Safe-T user. Price for 501-1,000 users.	$ 71.97

			Premises		
511210	SAFE-T	ZZPU-AN-2,500	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T user. Price for 1,001-2,500 users.	$ 65.16
511210	SAFE-T	ZZPU-AN-5,000	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T user. Price for 2,501-5,000 users.	$ 54.47
511210	SAFE-T	ZZPU-AN-10,000	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T user. Price for 5,001-10,000 users.	$ 41.82
511210	SAFE-T	ZZPU-AN-20,000	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T user. Price for 10,000-20.000 users.	$ 25.29
511210	SAFE-T	ZZPU-AN-30,000	ZoneZero SDP - Annual Enterprise Price on Premises	Safe-T user. Price for 20,000-30.000 users.	$ 15.56
511210	SAFE-T	Additional ZZ_SDP-AN-AGW	Additional ZZ_SDP-AN-AGW	ZoneZero Access & Authentication Gateway - Supporting up to 5,000 concurrent connection	$ 1,458.77
511210	SAFE-T	ZZ_SDP-AN-NonProd	ZZ_SDP-AN-NonProd	Additional Authentication Gateway - Supporting up to 5,000 concurrent connection	$ 2,431.27
511210	SAFE-T	ZZ-VPNM-AN	ZoneZero VPN - Annual SMB Price on	VPN integration	$ 2,723.03

			Premises		
511210	SAFE-T	ZZ-SSLM-AN (User Portal) interface Module	ZoneZero VPN - Annual SMB Price on Premises	User Portal interface Module	$ 2,139.52
511210	SAFE-T	ZZU-AN-49	ZoneZero VPN - Annual SMB Price on Premises	Safe-T user. Price for 25-49 users. (Includes 1 Access Controller & 1 gateway node). Supporting up to 5,000 concurrent connection	$ 73.91
511210	SAFE-T	ZZU-AN-100	ZoneZero VPN - Annual SMB Price on Premises	Safe-T user. Price for 50-100 users. (Includes 1 Access Controller & 1 gateway node). Supporting up to 5,000 concurrent connection	$ 71.00
511210	SAFE-T	ZZU-AN-250	ZoneZero VPN - Annual SMB Price on Premises	Safe-T user. Price for 101-250 users. (Includes 1 Access Controller & 1 gateway node). Supporting up to 5,000 concurrent connection	$ 63.21
511210	SAFE-T	ZZU-AN-500	ZoneZero VPN - Annual SMB Price on Premises	Safe-T user. Price for 251-500 users. (Includes 1 Access Controller & 1 gateway node). Supporting up to 5,000 concurrent connection	$ 53.49
511210	SAFE-T	ZZ_VPN-Server-PAN-AGW	ZoneZero VPN - Annual Enterprise Price on Premises	Safe-T ZoneZero virtual appliance *(Includes 1 Access Controller & 1 gateway node). Supporting up to 5,000 concurrent connection	$ 9,627.87
511210	SAFE-T	ZZ-VPNM-AN	ZoneZero VPN - Annual Enterprise Price on Premises	VPN integration	$ 2,723.03

511210	SAFE-T	ZZU-AN-1,000	ZoneZero VPN - Annual Enterprise Price on Premises	Safe-T user. Price for 501-1,000 users.	$ 50.57
511210	SAFE-T	ZZU-AN-2,500	ZoneZero VPN - Annual Enterprise Price on Premises	Safe-T user. Price for 1,001-2,500 users.	$ 43.76
511210	SAFE-T	ZZU-AN-5,000	ZoneZero VPN - Annual Enterprise Price on Premises	Safe-T user. Price for 2,501-5,000 users.	$ 35.98
511210	SAFE-T	ZZU-AN-10,000	ZoneZero VPN - Annual Enterprise Price on Premises	Safe-T user. Price for 5,001-10,000 users.	$ 27.23
511210	SAFE-T	ZZ-AN-NonProd	Additional ZoneZero Access Controller	Additional ZoneZero Access Controller	$ 2,431.27
511210	SAFE-T	ZZ_VPN-AN-Server-AGW-HA	Safe-T ZZ - Non Production, HA or DR - Annual	Safe-T ZZ - Non Production, HA or DR - Annual	$ 2,431.27
511210	SAFE-T	ZZPU-AN-49	ZoneZero SFA - Annual SMB Price on Premises	Safe-T user. Price for 25 - 49 users. (Includes Secure File Access Server)	$ 101.14
511210	SAFE-T	ZZPU-AN-100	ZoneZero SFA - Annual SMB Price on Premises	Safe-T user. Price for 50-100 users. (Includes Secure File Access Server)	$ 97.26

511210	SAFE-T	ZZPU-AN-250	ZoneZero SFA - Annual SMB Price on Premises	Safe-T user. Price for 101-250 users. (Includes Secure File Access Server)	$ 89.47
511210	SAFE-T	ZZPU-AN-500	ZoneZero SFA - Annual SMB Price on Premises	Safe-T user. Price for 251-500 users. (Includes Secure File Access Server)	$ 79.74
511210	SAFE-T	SFA-PAN	ZoneZero SFA - Annual Enterprise Price on Premises	Secure File Access Server – Annual	$ 9,725.11
511210	SAFE-T	ZZPU-AN-1,000	ZoneZero SFA - Annual Enterprise Price on Premises	Safe-T user. Price for 501-1,000 users.	$ 71.97
511210	SAFE-T	ZZPU-AN-2,500	ZoneZero SFA - Annual Enterprise Price on Premises	Safe-T user. Price for 1,001-2,500 users.	$ 65.16
511210	SAFE-T	ZZPU-AN-5,000	ZoneZero SFA - Annual Enterprise Price on Premises	Safe-T user. Price for 2,501-5,000 users.	$ 54.47
511210	SAFE-T	ZZPU-AN-10,000	ZoneZero SFA - Annual Enterprise Price on Premises	Safe-T user. Price for 5,001-10,000 users.	$ 41.82
511210	SAFE-T	ZZPU-AN-20,000	ZoneZero SFA - Annual Enterprise Price on	Safe-T user. Price for 10,000-20.000 users.	$ 25.29

			Premises		
511210	SAFE-T	ZZPU-AN-30,000	ZoneZero SFA - Annual Enterprise Price on Premises	Safe-T user. Price for 20,000-30.000 users.	$ 15.56
511210	SAFE-T	SFA-AN-NonProd	SFA-AN-NonProd	Safe-T SFA - Non Production, Additional SFA server	$ 2,431.27
54151	SAFE-T	ST-SL1	Partner Support Level 1	Provides: * 5 days a week, 8 hours a day (in your local time zone) * No onsite support * Safe-T support will be determined by the company SLA: **https://www.safe-t.com/wp-content/uploads/2020/06/SLA-Safe-T-Group-vJune2020.pdf**	3% of sale total
54151	SAFE-T	ST-SL2	Partner Support Level 2	Provides: * 7 days a week, 24 hours a day support * No onsite support Safe-T support will be determined by the company SLA: **https://www.safe-t.com/wp-content/uploads/2020/06/SLA-Safe-T-Group-vJune2020.pdf**	3% of sale total

Contracts Administrator:

Steven Reinkemeyer

President/CEO

703-229-6709

gsa@redport-ia.com

Safe-T End User License Agreement

This End User License Agreement ("Agreement") together with any other agreements or terms incorporated by reference, including the purchase order entered into between the Government customer, the Ordering Activity, under GSA Schedule contracts identified in the Purchase Order, Statement of Work, or similar document (the "**Licensee**") and SAFE-T. The Purchase Order, Statement of Work, or similar document (the "**PO**") govern Licensee's use of the proprietary software products (the "**Software**"). specified in the PO. This Agreement constitutes a binding and enforceable legal contract betweenLicensee and Safe-T Data A.R, Ltd. ("**SAFE-T**" and each of SAFE-T and Licensee a "**Party**" and collectively the "**Parties**").

1. License Rights

1.1 Installation and Use. Subject to payment of the applicable fees and compliance with the terms and conditions herein, SAFE-T grants to Licensee a revocable, non-exclusive and non-transferable (in whole or in part) license and right to install and use the Software during the Term, in object code executable form only, subject to the following use restrictions:

(a) The Software is licensed on a per-server and per-user basis, and limited to the number of users set forth in the PO, who are employees, consultants or agents of Licensee ("**Authorized Users**"). Access to the Software by persons other than Authorized Users will constitute a material breach of this Agreement.

(b) Installation and continuous use of the Software requires one or more license keys, which will be issued by SAFE-T to Licensee, and contain license related data that is recognized by the Software for automated license management purposes.

(c) Licensee shall ensure that all Authorized Users comply with the terms of this Agreement, and Licensee shall be liable for any violation of this Agreement by an Authorized User.

1.2 Additional Limitations.

(a) The license to use the Software is not transferable or assignable in whole or in part by Licensee and no license is granted to any user who did not originally purchase the applicable license for the Software from SAFE-T.

(b) Licensee acknowledges and agrees that certain software components of the Software are accompanied by license agreements containing terms which are different than this Agreement. Any third-party agreements are supplied with such third party software components, either electronically in a "license.txt" file in the root directory of the installation media, or the subdirectory in the installation media containing the third party software components. In any such situation, the third-party software components are supplied solely in accordance with the associated third party agreements. By executing this agreement, Licensee does not agree to be bound by any Third Party or additional terms without executing an agreement in writing. Licensee acknowledges that third party software has different terms.

(c) Licensee acknowledges and agrees that server external tools, if applicable, are implemented and designed based on application programming interface (APIs) provided by third-party application vendors at the time of their release. The execution of a third-party application upgrade and/or cumulative updates, without prior consultation with SAFE-T, may cause unexpected Software platform behavior.

(d) Licensee may not (i) modify, alter, create derivative works from, reverse engineer, decompile, or disassemble the Software, nor attempt in any other manner to obtain the source code; (ii) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; or (iii) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of SAFE-T.

(e) Licensee may not, whether through deliberate or negligent act or act of omission, distribute or cause the distribution of the Software to any third party other than an Authorized User, except that an Authorized User may provide a SAFE-T smart transfer agent and a SAFE-T outlook plugin to an external user.

(f) Licensee may not disseminate, distribute, disclose, or copy the printed documentation that accompanies the Software.

(g) Licensee may not sublicense, rent, or lease any portion of the Software.

(h) Licensee may not use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement.

(i) Licensee may not use a previous version or copy of the Software after it has received and installed an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed.

(j) Licensee may not use the Software in any manner not expressly authorized by this Agreement.

2. Proprietary Rights; Feedback

2.1 Ownership. All rights, title, interest and intellectual property rights in and to the Software, the accompanying documentation, and any copies of the Software, or any derivatives thereof, are owned by SAFE-T or its licensors. The Software is protected by copyright laws, other intellectual property rights and international treaty provisions. Accordingly, Licensee is required to treat the Software like any other copyrighted material and nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software, except as otherwise allowed pursuant to this Agreement and that it may make copies of the Software solely for backup or archive purposes. Licensee acknowledges that the Software, any product in which the Software is embedded and Documentation contain intellectual property rights (such as international and United States copyrights, patents, and patents pending) of SAFE-T. Safe-T's technology, Software and any product in which the Software is embedded are covered by one or more issued or pending patents, as more fully detailed on the Patent Notice page of SAFE-T's website here: https://www.safe-t.com/the-safe-t/, as well as issued and pending international patents.

2.2 Feedback. Licensee may, but is not obligated to, provide to SAFE-T any suggestions, comments and feedback regarding the Software (collectively, "**Licensee Feedback**"). SAFE-T may use and include any Licensee Feedback that Licensee voluntarily provides to improve the Software or other related SAFE-T technologies. Accordingly, if Licensee provides Licensee Feedback, Licensee grants SAFE-T and its Licensees a perpetual, irrevocable, worldwide, royalty-free, fully paid-up license grant to freely use, have used, sell, modify, reproduce, transmit, license, sublicense (through multiple tiers of sublicensees), distribute (through multiple tiers of distributors), and otherwise commercialize the Licensee Feedback in the Software or other related technologies. Licensee Feedback and shall be considered SAFE-T's Confidential Information. SAFE-T acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

3. Audit Rights

3.1 SAFE-T reserves the right to audit Licensee's use of the Software, no more than once annually, during the Term of this Agreement and thereafter at SAFE-T's expense. Licensee shall allow SAFE-T or its agents to access Licensee's computer systems and physical facilities for such audit, subject to applicable Government security requirements. Audit shall be conducted during normal business hours at Licensee'sfacilities and shall not unreasonably interfere with Licensee'sbusiness activities.

4 Limited Warranty; Limitation of Liability

4.1 Subject to the terms and conditions herein, SAFE-T warrants that the Software will conform to its specifications in the documentation provided therewith for a period of one (1) year from the date of installation at the Licensee site (the "**Warranty Period**"). The warranty stated hereinabove shall be at all times contingent upon Licensee's proper use of the Software, and shall not apply to damage or defect caused by misuse, alteration, or unauthorized repair, integration or installation, other than as stated in the related documentation, or the execution of a third-party application upgrade and/or cumulative updates, without prior consultation with SAFE-T. Subject to the aforementioned, if the Software does not perform as warranted during the Warranty Period, SAFE-T's sole and exclusive liability shall be to make commercially reasonable efforts to repair or replace such non-conforming Software. SAFE-T does not warrant that the Software will meet Licensee's requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

4.2 TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

4.3 EXCEPT WITH RESPECT TO CLAIMS ARISING UNDER SECTION 5 (INDEMNIFICATION) TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SAFE-T BE LIABLE UNDER OR IN CONNECTION WITH THIS AGREEMENT FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SAFE-T HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.4 EXCEPT WITH RESPECT TO CLAIMS ARISING UNDER SECTION 5 (INDEMNIFICATION) IN NO EVENT SHALL SAFE-T'S AGGREGATE LIABILITY FOR ANY AND ALL DAMAGES, LOSSES AND CLAIMS ARISING UNDER OR RELATING TO THIS AGREEMENT EXCEED THE AMOUNT OF MONEY ACTUALLY PAID BY LICENSEE UNDER THE PO. THE LIMITATIONS OF SAFE-T'S LIABILITY SET FORTH IN THIS SECTION SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY OF THE LIMITED REMEDIES SET FORTH HEREIN.

4.5 THIS AGREEMENT DOES NOT LIMIT OR DISCLAIM ANY OF THE WARRANTIES SPECIFIED IN THE GSA SCHEDULE 70 CONTRACT UNDER FAR 52.212-4(O). IN THE EVENT OF A BREACH OF WARRANTY, THE U.S. GOVERNMENT RESERVES ALL RIGHTS AND REMEDIES UNDER THE CONTRACT, THE FEDERAL ACQUISITION REGULATIONS, AND THE CONTRACT DISPUTES ACT, 41 U.S.C. 7101-7109.

4.6 THIS AGREEMENT SHALL NOT IMPAIR THE U.S. GOVERNMENT'S RIGHT TO RECOVER FOR FRAUD OR CRIMES ARISING OUT OF OR RELATED TO THIS CONTRACT UNDER ANY FEDERAL FRAUD STATUTE, INCLUDING THE FALSE CLAIMS ACT, 31 U.S.C. 3729-3733. FURTHERMORE, THIS CLAUSE SHALL NOT IMPAIR NOR PREJUDICE THE U.S. GOVERNMENT'S RIGHT TO EXPRESS REMEDIES PROVIDED IN THE GSA SCHEDULE CONTRACT (E.G., CLAUSE 552.238-75 – PRICE REDUCTIONS, CLAUSE 52.212-4(H) – PATENT INDEMNIFICATION, AND GSAR 552.215-72 – PRICE ADJUSTMENT – FAILURE TO PROVIDE ACCURATE INFORMATION).

4.7 The limited warranty, limited remedies, warranty disclaimer and limitation of liability are fundamental elements of the basis of the transaction between SAFE-T and Licensee. SAFE-T would not be able to provide the software without suchlimitations.

5 Indemnification.

5.1 SAFE-T will have the right to intervene to defend, indemnify and hold Licensee harmless, from and against all finally awarded claims, actions, suits or proceedings (collectively, "**Claims**"), and pay all resulting losses, liabilities, damages, settlement amounts costs or expenses (including attorney's fees) (collectively, "Losses"), incurred by Licensee resulting from or in connection with any claims by third parties that the Software infringes any intellectual property right provided that SAFE-T is notified promptly of such claim and is given full and authority (including settlement authority), information and assistance by Licensee for such defense. 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. In the event that the Software is held in connection with any such claim to infringe such a right and its use is enjoined, or if in the opinion of SAFE-T the Software is likely to become the subject of such a claim, SAFE-T will either, in its sole discretion (i) procure for Licensee the right to continue using the Software, or (ii) modify or replace the Software so that it becomes non-infringing while giving substantially equivalent performance. In the event that (i) or (ii) above are not, in SAFE-T's sole reasonable determination, obtainable using commercially reasonable efforts, then SAFE-T may terminate this Agreement and refund the amount the Licensee has paid SAFE-T under this Agreement for the Software that is the subject of such claim. This section states Licensee's exclusive remedy and SAFE-T's entire liability for any claim ofinfringement.

6 Term and Termination

6.1 Term. This Agreement will enter into effect on the date specified in the PO (the "**Effective Date**") and will remain in force for the period specified in the PO unless terminated pursuant to Section 6.2(the "**Term**").

6.2 Revocation of License. In the event that this Agreement is terminated in accordance with Section 8.2, the Support Services and all licenses granted to Licensee hereunder will terminate immediately andLicensee shall: (i) immediately remove all copies of the Software from all computers in Licensee's control and (ii) immediately return all copies of the Software or certify the destruction or deletion thereof. SAFE-T shall have the right to have an inspection and audit of Licensee to confirm removal and destruction of the Software subject to Government security requirements.

6.3 Survival. The provisions of sections 1 (License Rights), 1.22 (Proprietary Rights; Feedback), 3 (Audit Rights), 4 (Limited Warranty; Limitation of Liability), 5 (Indemnification), 6 (Term and Termination), 7 (Confidential Information; Access to Software) and 9 (General Provisions)shall survive termination or expiration of this Agreement.

7 END-OF-LIFE

SAFE-T reserves the right to end-of-life (EOL) the Software three (3) years after the end-of-sale date. If you prepaid the fee for the Software which is subject to EOL, SAFE-T will use commercially reasonable efforts to transition you to a substantially similar Software. If SAFE-T does not have asubstantially similar Software, then SAFE-T will credit you anyunused portion of the prepaid fee for such Software, calculated from the last date the SAFE-T Software is available.

8 Confidential Information; Access to Software

8.1 "**Confidential Information**" shall mean any information, technical data, or know-how, in written, graphic, machine readable form or any other form, including but not limited to information which may relate to past, present and future research, product plans, products (including the Software) or services of SAFE-T, and including any unannounced products or services of SAFE-T, the Software and the documentation relating to the Software or any part or derivative thereof, that is disclosed to or learned by Licensee in connection with this Agreement. When the end user is the Federal Government, neither this Agreement nor the pricing terms are confidential information notwithstanding any such markings.

8.2 Licensee shall not use or disclose any Confidential Information except as expressly authorized by this Agreement, and shall protect all such Confidential Information using the same degree of care which Licensee uses with respect to its own proprietary information of similar importance, but in no event with safeguards less than a reasonably prudent business would exercise under similar circumstances. Licensee shall not use the Confidential Information for any purpose other than as strictly needed to exercise its rights under this Agreement. The transfer of Confidential Information to Licensee does not grant Licensee any ownership or license rights are in any Confidential Information. Licensee shall use commercially reasonable efforts to prevent any actual or threatened unauthorized copying, use or disclosure of Confidential Information, and shall promptly notify SAFE-T of any such actual or threatened unauthorized disclosure or use. SAFE-T 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 SAFE-T. If any Confidential Information must be disclosed to any third party by reason of legal, accounting or regulatory requirements beyond the reasonable control of Licensee, Licensee shall promptly notify SAFE-T of the order or request and permit SAFE-T (at its own expense) to seek an appropriate protective order.

9 General Provisions

9.1 Severability. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remainder of this Agreement will continue in full force and effect. This Agreement has been negotiated by the parties and their respective counsel and will be interpreted fairly in accordance with its terms and without any strict construction in favor of or against either party.

9.2 Amendments. The Agreement shall not be modified except by a written agreement that names this Agreement and any provision to be modified, is dated subsequent to the Effective Date, and is signed by duly authorized representatives of both parties.

9.3 No Waiver. No failure or delay on the part of either party in the exercise of any right, power or remedy under this Agreement or under law shall operate as a waiver thereof, nor shall any single or partial exercise of any right, power or remedy preclude other or further exercise thereof, or the exercise of any other right, power or remedy.

9.4 No Assignment. This Agreement, and Licensee's rights and obligations herein, may not be assigned or otherwise transferred by Licensee without SAFE-T's prior written consent, and any attempted assignment in violation of the foregoing will be null and void. The terms of this Agreement shall be binding upon the parties' respective assignees.

9.5 Independent Contractors. SAFE-T's relationship to Licensee is that of an independent contractor, and neither party is an agent or partner of the other. Neither party will have, or will represent to any third party that it has, any authority to act on behalf of the other party.

9.6 Export Restrictions. The parties acknowledge that the Software is subject to U.S. and Israeli export control laws and regulations. The parties agree to comply with all applicable international and national laws that apply to the Software, including the Israeli Export Control Laws and U.S.Export Administration Regulations, as well as end-user, end-use and destination restrictions issued by U.S. and other governments. Under no circumstances may Software be exported to: Cuba, Iran, North Korea, Sudan and Syria or any location in control thereof. The parties hereto further warrant that they are not on the U.S Treasury Department list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders.

9.7 Counterparts. This Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which together shall constitute one instrument.

9.8 No Third Party Beneficiaries. This Agreement is solely between SAFE-T and Licensee. There are no third partybeneficiaries, express or implied, to this Agreement.

9.9 Entire Agreement. This Agreement, together with the underlying GSA Schedule Contract, Schedule Pricelist and PO constitutes the entire agreement between the parties with respect to the subject matter contemplated herein, and merges all prior and contemporaneous communications. Specifically, in the event of any conflict between this Agreement and any click-wrap or shrink-wrap provisions accompanying the Software, the terms of this Agreement shall prevail, notwithstanding anything to the contrary contained in the click/shrink wrap provisions.

***