GENERAL SERVICES ADMINISTRATION

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.

Multiple Award Schedule

FSC Group: Information Technology
FSC Class:

Contract number: **47QTCA18D001N**

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

Contract period: **10/31/2022-10/30/2027**

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

www.redport-ia.com

Contract Administrator:
Steven P Reinkemeyer
gsa@redport-ia.com
Phone: 703-229-6709

Business size: Small Business, Service Disabled Veteran Owned Small Business

Price list current as of Modification #: PS-0017 – Effective 11/17/2022

CUSTOMER INFORMATION

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

SIN	Description
54151S	IT Professional Services
54151	Software Maintence Services
511210	Software Licenses
54151HACS	Highly Adaptive Cybersecurity Services SUBCATEGORIES: • High Value Assessments • Risk and Vulnerability Assessments • Penetration Testing • Cyber Hunt • Incident Response
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 32***

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. ***See Page 5***

2. Maximum order: **$500,000**

3. Minimum order: $100

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

5. Point(s) of production (city, county, and State or foreign country). N/A

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(s) 54151S and SIN 54151HACS

8. Prompt payment terms. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions: NET 30

9. Foreign items (list items by country of origin). Not Applicable

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

10b. Expedited Delivery. Items available for expedited delivery are noted in this price list. Contact Contractor

10c. Overnight and 2-day delivery. Contact Contractor

10d. Urgent Requirements. Contact Contractor

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

12a. Ordering address(es).
Redport Information Assurance LLC
814 W Diamond Avenue. Ste. 370
Gaithersburg, MD 20878

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

13. Payment address(es).
Redport Information Assurance LLC
814 W Diamond Avenue. Ste. 370
Gaithersburg, MD 20878

14. Warranty provision. Standard Commercial Warranty Terms & Conditions

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). Not Applicable

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable). Not Applicable

18b. Terms and conditions for any other services (if applicable). Not Applicable

19. List of service and distribution points (if applicable). Not Applicable

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

21. Preventive maintenance (if applicable). Not Applicable

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/.
Not Applicable

23. Unique Entity Identifier (UEI) number: S3VMFSL92216

24. Notification regarding registration in System for Award Management (SAM) database.
Contractor registered and active in SAM

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,	Associates	2

	System Plan of Action and Milestones, IT Continuity Plan, Security Design Management Process, Security Requirements Traceability Matrix and other documentation to satisfy IA controls).		
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	Bachelors	4

	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).		
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	Bachelors	8

	security using penetration testing and red teams. Provides technologies for identification, modeling, and predictive analysis of cyber threats.		
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	Bachelors	4

	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.		
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.	Bachelors	6

	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.		
Cyber Security/Information Assurance Auditor	Provides an audit of security systems used. Provides a detailed report of information	Bachelors	6

	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.		
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,	Bachelors	6

	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.		
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	Bachelors	6

	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.		
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.	Bachelors	6

	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	Bachelors	6

	software. Analyzes, troubleshoots and corrects network problems remotely and on-site. Maintains and administers perimeter security systems such as firewalls and intrusion detection systems.		
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	Associates	2

	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.		
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,	Associates	2

	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.		

LABOR CATEGORY DESCRIPTIONS (54151HACS)

SUBCATEGORIES:

- HIGH VALUE ASSESSMENTS (HVA)
- RISK AND VULNERABILITY ASSESSMENTS (RVA)
- PENETRATION TESTING
- CYBER HUNT
- INCIDENT RESPONSE

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	Associates	2

	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).		
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	Bachelors	4

	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).		

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	Bachelors	6

	development, and/or company secrets.		
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

	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.		
Cyber Security Engineer II	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 information system contingency plans that maintain appropriate levels of protection and meet time	Bachelors	6

	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	Bachelors	6

	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.		
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	Bachelors	6

		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.		
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	Bachelors	6

	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, 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	Associates	2

	problems. Expected to quickly and accurately find a solution.		
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	Associates	2

	phases of the system development life cycle.		

LABOR CATEGORY RATES
(All rates below include IFF)

SIN	Labor Category	10/31/2022-10/30/2023	10/31/2023-10/30/2024	10/31/2024-10/30/2025	10/31/2025-10/30/2026	10/31/2026-10/30/2027
54151S	*C&A/A&A Analyst*	$ 99.91	$ 101.90	$ 103.94	$ 106.02	$ 108.13
54151S	*C&A/A&A Engineer*	$ 112.75	$ 115.00	$ 117.30	$ 119.65	$ 122.05
54151S	*Digital Forensics Engineer*	$ 161.38	$ 164.60	$ 167.90	$ 171.25	$ 174.68
54151S	*Penetration Tester*	$ 141.92	$ 144.77	$ 147.66	$ 150.61	$ 153.62
54151S	*Security SME*	$ 209.46	$ 213.65	$ 217.92	$ 222.29	$ 226.73
54151S	*Technical Writer*	$ 69.13	$ 70.51	$ 71.92	$ 73.36	$ 74.83
54151S	*Cyber Security Engineer II*	$ 125.62	$ 128.13	$ 130.69	$ 133.30	$ 135.97
54151S	*Information Assurance Specialist*	$ 186.61	$ 190.34	$ 194.15	$ 198.03	$ 201.98
54151S	*Cyber Security/Information Assurance Auditor*	$ 145.28	$ 148.18	$ 151.14	$ 154.17	$ 157.25
54151S	*Cyber Security Engineer III*	$ 168.88	$ 172.25	$ 175.70	$ 179.21	$ 182.80
54151S	*Security Software Engineer Team Lead*	$ 182.35	$ 185.99	$ 189.71	$ 193.51	$ 197.38
54151S	*Incident Response Lead*	$ 156.26	$ 159.39	$ 162.57	$ 165.82	$ 169.14
54151S	*Network Security Engineer III*	$ 168.88	$ 172.25	$ 175.70	$ 179.21	$ 182.80
54151S	*Cyber Security Program/Project Manager*	$ 189.48	$ 193.27	$ 197.14	$ 201.08	$ 205.10
54151S	*Security Administrator*	$ 76.50	$ 78.04	$ 79.60	$ 81.19	$ 82.81
54151S	*Cyber Security Engineer I*	$ 99.89	$ 101.88	$ 103.92	$ 105.99	$ 108.11
54151HACS	*C&A/A&A Analyst*	$ 99.91	$ 101.90	$ 103.94	$ 106.02	$ 108.13
54151HACS	*C&A/A&A Engineer*	$ 112.75	$ 115.00	$ 117.30	$ 119.65	$ 122.05
54151HACS	*Digital Forensics Engineer*	$ 161.38	$ 164.60	$ 167.90	$ 171.25	$ 174.68

54151HACS	*Penetration Tester*	$ 141.92	$ 144.77	$ 147.66	$ 150.61	$ 153.62
54151HACS	*Security SME*	$ 209.46	$ 213.65	$ 217.92	$ 222.29	$ 226.73
54151HACS	*Technical Writer*	$ 69.13	$ 70.51	$ 71.92	$ 73.36	$ 74.83
54151HACS	*Cyber Security Engineer II*	$ 125.62	$ 128.13	$ 130.69	$ 133.30	$ 135.97
54151HACS	*Information Assurance Specialist*	$ 186.61	$ 190.34	$ 194.15	$ 198.03	$ 201.98
54151HACS	*Cyber Security/Information Assurance Auditor*	$ 145.28	$ 148.18	$ 151.14	$ 154.17	$ 157.25
54151HACS	*Cyber Security Engineer III*	$ 168.88	$ 172.25	$ 175.70	$ 179.21	$ 182.80
54151HACS	*Security Software Engineer Team Lead*	$ 182.35	$ 185.99	$ 189.71	$ 193.51	$ 197.38
54151HACS	*Incident Response Lead*	$ 156.26	$ 159.39	$ 162.57	$ 165.82	$ 169.14
54151HACS	*Network Security Engineer III*	$ 168.88	$ 172.25	$ 175.70	$ 179.21	$ 182.80
54151HACS	*Cyber Security Program/Project Manager*	$ 189.48	$ 193.27	$ 197.14	$ 201.08	$ 205.10
54151HACS	*Security Administrator*	$ 76.50	$ 78.04	$ 79.60	$ 81.19	$ 82.81
54151HACS	*Cyber Security Engineer I*	$ 99.89	$ 101.88	$ 103.92	$ 105.99	$ 108.11

Rates and Descriptions for SIN 511210 Software Licenses and SIN 54151 Software Maintenance Services (All rates below include IFF)

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	$	23.34

				5,000 concurrent connection	
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 Premises	Safe-T user. Price for 501-1,000 users.	$ 71.97
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	Safe-T user. Price for 20,000-30.000 users.	$ 15.56

			Price on Premises		
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 Premises	VPN integration	$ 2,723.03
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	Safe-T user. Price for 101-250 users. (Includes 1 Access Controller & 1 gateway node). Supporting	$ 63.21

			on Premises	up to 5,000 concurrent connection	
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 Premises	Safe-T user. Price for 10,000-20.000 users.	$ 25.29
511210	SAFE-T	ZZPU-AN-30,000	ZoneZero SFA - Annual Enterprise	Safe-T user. Price for 20,000-30.000 users.	$ 15.56

			Price on Premises		
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

Service Contract Labor Standards: The Service Contract Labor Standards (SCLS), formerly known as the Service Contract Act (SCA), is applicable to this contract as it applies to the entire Multiple Award Schedule (MAS) and all services provided. While no specific labor categories have been identified as being subject to SCLS/SCA due to exemptions for professional employees (FAR 22.1101, 22.1102 and 29 CRF 541.300), this contract still maintains the provisions and protections for SCLS/SCA eligible labor categories. If and / or when the contractor adds SCLS/SCA labor categories to the contract through the modification process, the contractor must inform the Contracting Officer and establish a SCLS/SCA matrix identifying the GSA labor category titles, the occupational code, SCLS/SCA labor category titles and the applicable WD number. Failure to do so may result in cancellation of the contract.