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 is available through **GSA** *Advantage*!™, a menu-driven database system. The INTERNET address for **GSA** *Advantage*!™ is: **http://www.GSAAdvantage.gov.**

Multiple Award Schedule (MAS)

Federal Supply Group: Information Technology

Contract Number: GS-35F-424AA

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

Contract Period: June 18, 2013 – June 17, 2023

Price List current as of Modification #PA-0026 Effective May 13, 2020

Contractor:

Sev1Tech, LLC.
12700 Black Forest Lane, Ste 306
Woodbridge, VA 22192

Business Size: Large Business

Telephone: (703) 662-9778
FAX Number:
Web Site: www.sev1tech.com
E-mail: Kate.Giebler@sev1tech.com
Contract Administration: Kathryn Giebler

CUSTOMER INFORMATION:

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

SIN	SIN Description	Page #
54151S	Information Technology (IT) Professional Services	4
518210C	Cloud and Cloud-Related IT Professional Services	10
54151HACS	Highly Adaptive Cybersecurity Services (HACS)	42

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. – N/A

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 labor category descriptions for the following:

54151S – Page 8
518210C – Page 16
54151HACS -

2. Maximum Order: $500,000.00

3. Minimum Order: $100.00

4. Geographic Coverage (delivery Area): Domestic and Worldwide

5. Point(s) of production (city, county, and state or foreign country): Same as company address

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

7. Quantity discounts: None

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

9. Foreign items (list items by country of origin): None

10a. Time of Delivery (Contractor insert number of days): Specified on the Task Order

10b. Expedited Delivery. Contact Contractor

10c. 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

10d. Urgent Requirements. Contact Contractor

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

12a. Ordering Address(es): Same as Contractor

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

13. Payment address(es): Same as company address

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

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

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

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

18a. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): N/A

18b. Terms and conditions for any other services (if applicable): N/A

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

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

21. Preventive maintenance (if applicable): N/A

22a. Special attributes such as environmental attributes (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A

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

23. Data Universal Numbering System (DUNS) number: 962121286

24. Notification regarding registration in System for Award Management (SAM database: Registered

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

1.1. SCOPE

a. The prices, terms and conditions stated under Special Item Numbers 54151S 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.

1.2. 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.

1.3. 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 Agreement; 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.

1.4. 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 Regulation, 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.

1.5. STOP-WORK ORDER (FAR Sl.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. l11e order shall be specifically identified as a stop-work order is used under this clause. Upon receipt of the order, the Contractor shall immediately comply with its tem1s 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-

   i. Cancel the stop-work order; or

   ii. 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-

   i. 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

   ii. 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.

1.6. INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS-COMMERCIAL ITEMS (MAR 2009) (DEVJATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS -COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I - OCT 2008) {DEVIATION I - FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract

1.7. RESPONSIBILITIESOFTHE 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.

1.8. RESPONSIBILITIESOF 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.

1.9. 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.

1.10. 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.

1.11. INVOICES

The Contractor, upon completion of the work ordered, shalt submit invoices for IT Professional services. Progress payment'! 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.

1.12. 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. S2.216-3l(Feb 2007) Time- and-Materials/Labor-Hour Proposal Requirements-Commercial Item Acquisition As prescribed in 16.60l(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-

   i. The offeror;
   ii. Subcontractors; and/or
   iii. Divisions, subsidiaries, or affiliates of the offeror under a common control.

1.13. RESUMES

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

1.14. 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.

1.15. 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.

1.16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

a. Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151S 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.

Labor Category	Rate
Analyst I	$69.94
Analyst II	$84.88
Cyber Security Architect Ill	$147.57
Cyber SME V	$148.10
Cyber SME VI	$166.37
Network SME IV	$160.94
Network SME V	$207.34
Platform SME IV	$143.17
Platform SME V	$197.47
Security Systems Integration Engineer	$222.15
Senior Firewall Engineer	$207.34
Senior Subject Matter Expert III	$122.08
Senior Subject Matter Expert IV	$147.21
Senior Tech PM IV	$146.67
Staff Consultant	$84.77
Subject Matter Expert I	$99.28
Subject Matter Expert II	$112.63
Subject Matter Expert V	$188.58
Systems Engineer 5	$167.85
Systems Engineer 6	$188.58
Technical Delivery Manager II	$133.78

1.17 SIN 54151S LABOR CATEGORY DESCRIPTIONS

Unless otherwise stated, experience and education may be substituted for each other on a year for year basis.

GSA Labor Title	Functions	Edu	Exp
Analyst I	Responsible for reporting directly to Project and/or Program Managers and may require interfacing with the client in direct support of program efforts. Participate in all aspects of project schedule planning, development, delivery and maintenance in support of complex IT program and/or projects. Able to update, maintain schedules, record meeting minutes, and provide documentation and PM documents. Participates in the coordination of the individual projects and activities into a successful overall Program schedule. Can take initiative and maintain confidentiality while multi-tasking in a fast-paced team-oriented environment.	Bachelors	1
Analyst II	Responsible for reporting directly to Project and/or Program Managers and may require interfacing with the client in direct support of program efforts. Participate in all aspects of project schedule planning, development, delivery and maintenance in support of complex IT program and/or projects. Able to update, maintain schedules, record meeting minutes, and provide documentation and PM documents. Participates in the coordination of the individual projects and activities into a successful overall Program schedule. Can take initiative and maintain confidentiality while multi-tasking in a fast-paced team-oriented environment.	Bachelors	3
Cyber Security Architect III	Responsible for leading security initiatives relating to information Assurance (IA) with the design/deployment/maintenance of new and field existing security infrastructure capabilities. Provides technical direction in the areas of vulnerability assessment risk assessment. network, security, product evaluation, and security implementation. Designs contingency plans of information Systems in order to maintain appropriate levels of protection and meet time requirements for minimizing operations impact to a customer's organization. Follows and ensuring compliance with federal security regulations and guidelines while making improvement recommendations to the customer. Able to design project roadmaps for IT architecture in support of business change projects	Masters	3
Cyber SME V	Installs software, such as firewalls, to protect computer networks. Plan and carry out security measures to protect an organization's computer networks and systems. Responsibilities are continually expanding as the number of cyberattacks increases. Help prevent attacks through their expertise and knowledge of databases, networks, hardware, firewalls and encryption. ... May also regulate access to computer files, develop firewalls, perform risk assessments and test data processing systems to verify security measures Plan, implement and upgrade security measures and controls Establish plans and protocols to protect digital files and information systems against unauthorized access, modification and/or destruction Maintain data and monitor security access Perform vulnerability testing, risk analyses and security assessments Conduct internal and external security audits Anticipate security alerts, incidents and disasters and reduce their likelihood Manage network, intrusion detection and prevention systems Analyze security breaches to determine their root cause Recommend and install appropriate tools and countermeasures Define, implement and maintain corporate security policies Train fellow employees in security awareness and procedures Coordinate security plans with outside vendors.	Bachelors	8

GSA Labor Title	Functions	Edu	Exp
Cyber SME VI	Installs software, such as firewalls, to protect computer networks. Plan and carry out security measures to protect an organization's computer networks and systems. Responsibilities are continually expanding as the number of cyberattacks increases. Help prevent attacks through their expertise and knowledge of databases, networks, hardware, firewalls and encryption. ... May also regulate access to computer files, develop firewalls, perform risk assessments and test data processing systems to verify security measures Plan, implement and upgrade security measures and controls Establish plans and protocols to protect digital files and information systems against unauthorized access, modification and/or destruction Maintain data and monitor security access Perform vulnerability testing, risk analyses and security assessments Conduct internal and external security audits Anticipate security alerts, incidents and disasters and reduce their likelihood Manage network, intrusion detection and prevention systems Analyze security breaches to determine their root cause Recommend and install appropriate tools and countermeasures Define, implement and maintain corporate security policies Train fellow employees in security awareness and procedures Coordinate security plans with outside vendors	Bachelors	10
Network SME IV	Installs, maintains and evaluates network systems and communications. Troubleshoots the complex network issues involving various factors. Conducts network architecture design, feasibility and cost studies. Must have extensive knowledge of Internet, computer, routers, switches, firewall, etc. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.	Bachelors	8
Network SME V	Installs, maintains and evaluates network systems and communications. Troubleshoots the most complex network issues. Conducts various researches and analysis regarding new technology, network traffic, potential security risk, etc. Leads the network architecture design and optimization. Must have extensive knowledge of Internet, computer, routers, switches, firewall, etc. Typically reports to a manager. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution or project goal terms. May provide a leadership role for the work group through knowledge in the area of specialization.	Bachelors	10
Platform SME IV	Participate in and support the conduction of deliberate planning for Platform Information Technology (PIT) or control systems in support of user action officers. Apply advanced knowledge of network architecture and operations to analyze and define solutions. Assess threats and vulnerabilities and recommend appropriate strategies to defend or exploit them. Maintain thorough knowledge of platform operations and operations community architecture. Assess operational risks and issues, develop effective courses of action and mitigation strategies, and coordinate actions for planning in support user operational planning process activities. Use engineering methodologies to develop concepts for assessing system resilience.	Bachelors	5
Platform SME V	Participate in and support the conduction of deliberate planning for Platform Information Technology (PIT) or control systems in support of user action officers. Apply advanced knowledge of network architecture and operations to analyze and define solutions. Assess threats and vulnerabilities and recommend appropriate strategies to defend or exploit them. Maintain thorough knowledge of platform operations, operations community architecture and drives efficiencies in operations and maintenance. Assess operational risks and issues, develop effective courses of action and mitigation strategies, and coordinate actions for planning in support user operational planning process activities. Use engineering methodologies to develop concepts for assessing system resilience. Coordinate planning efforts across members of the user community and access current scientific and technical intelligence products for awareness of threats to systems.	Bachelors	7

GSA Labor Title	Functions	Edu	Exp
Security Systems Integration Engineer	Develops and implements solutions integrating applications across the enterprise or its units/departments. This role may identify or resolve highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to continue as normal. The Security Systems Integration Engineer designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Performs more routine aspects of the position and is supervised by higher levels. Evaluates existing components or systems to determine integration requirements and to ensure final solutions meet organizational needs. Requires C++ or Java; XML; EDI or OBI; Oracle or Microsoft SQL. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.	Bachelors	5
Senior Firewall Engineer	Firewall engineers design, build, and manage the security infrastructure of information technology (IT) systems. This includes installing hardware, configuring firewalls, setting up virtual private networks (VPNs), and adding upgrades. Despite the strong technical focus of the job, firewall engineers also engage with clients, relaying information about the project and troubleshooting all issues discovered. They are proficient in change management and disaster response, and they actively apply policies and standards to all projects. While they spend most of their time in front of a computer, they often function within a team of other engineers, and they may work shifts at irregular hours to perform maintenance at unobtrusive times or resolve critical issues.	Bachelors	6
Senior Subject Matter Expert III	Subject Matter Expertise in a technical field in a technical field or specialized engineering or technology integration area and is proficient in relevant engineering principles. Applies experience skills. And expert knowledge within an engineering discipline to complex assignments. Generates unique concepts as evidenced by synthesis of new products or processes. Provides leadership for engineering activities in a specialized engineering or technology subject area. Serves as a major contributor to technical planning processes and for providing technical management and guidance.	Bachelors	8
Senior Subject Matter Expert IV	Expert in Single or Multiple technical disciplines providing expert knowledge from both commercial of specialization and federal experience and insight into specific areas of effective IT engineering and operations. Guides the development and application of this knowledge to the project. independently performs a variety of system design and integration tasks where subject matter expertise is required.	Bachelors	10
Senior Tech PM IV	Providing overall direction, control, and reporting of multiple projects with the ability to provide technical and management guidance to ensure all schedule and cost objectives are successfully achieved. Able to track and manage resources on the project. Responsible for establishing project plans, budgets, schedules, and documentation of work results. Able to coordinate with team, vendors, and stakeholders to ensure that all necessary deliverables and activities are completed on schedule and within the designated budget. Resolve issues (both technical and design) and recommend solutions. Able to deliver business value to customers by implementing effective information systems solutions that address the customer's business problems, needs and opportunities, in a manner consistent with the client strategic and business goals.	Bachelors	10
Staff Consultant	Assists teams with routine data gathering and research activities, organizes data and project documents, and assists project managers with project administrative activities. Ability to prepare briefings, web content, technical or process documents, and provide technical editing. Provides analytical and writing support to prepare, edit, and develop professional deliverables. Works directly with customers to define needs, develop solutions, and plan work. Uses experience and knowledge in field to formulate innovative and practical solutions. Performs complex tasks without supervision, and is typically supervised by a Senior Consultant or Project Manager.	Bachelors	4

GSA Labor Title	Functions	Edu	Exp
Subject Matter Expert I	Develops requirements from a project's inception to its conclusion in the subject matter area for simple to moderately complex systems. Assists senior team members with analysis and evaluation and with the preparation of recommendations for system improvements, optimization, development, and/or maintenance efforts in the following specialties: information systems architecture; networking: telecommunications: automation; communications protocols; risk management/electronic analysis; software; life-cycle management; software development methodologies: and modeling and simulation.	Bachelors	2
Subject Matter Expert II	Provides Functional and/or process expertise and skills relevant to a specific specialized domain area. Has a strong understanding of every step within the full life cycle development process. Experienced in the operational environment and using high-level functional systems analysis, design, integration, documentation, and implementation methodologies on complex problems that require in-depth knowledge of the subject matter for effective implementation. Applies principals, methods, and knowledge to the functional area of expertise to specific order requirements. Plans and prepares technical reports. data bases, studies, and related documentation, makes charts and graphs to record results. Prepares and delivers briefings as required by the order.	Bachelors	4
Subject Matter Expert V	An SME has proficiency in his or her subject and guides other professionals on the project to ensure the content is accurate. A subject matter expert (SME) is an individual who is considered an expert on particular subjects, or flagged as an expert in a piece of management software or other technology. The subject matter expert has a particular territory in which he or she has demonstrated above-average knowledge or experience. A subject matter expert is an individual with a deep understanding of a particular process, function, technology, machine, material or type of equipment. Individuals designated as subject matter experts are typically sought out by others interested in learning more about or leveraging their unique expertise to solve specific problems or help meet particular technical challenges. Subject matter experts in some fields often serve as expert witnesses in lawsuits and other legal actions.	Masters	12
Systems Engineer 5	Plans and designs an organization's systems infrastructure, including the implementation and design of hardware and software. Analyzes, develops, modifies, tests and maintains the system. Verifies and validates systems and meets internal and external requirements. Diagnoses problems and provides recommendations for improvement on existing and new systems. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.	Bachelors	8
Systems Engineer 6	Leads the planning and designing of an organization's systems infrastructure. Ensures the accuracy and effectiveness of the system meet business/customers' requirements. Monitors the performance of systems and suggests improvements. Verifies and reviews system related documents/reports including installation procedures. Typically reports to a manger or head of unit/department. Works on advanced, complex technical projects or business issues requiring state of the art technical or industry knowledge. Works autonomously. Goals are generally communicated in solution or project goal terms. May provide a leadership role for the work group through knowledge in the area of specialization.	Bachelors	10
Technical Delivery Manager II	Responsible for engineering teams and managing technical projects on time and within budget. Participate in all aspects of project schedule planning, development, delivery and maintenance in support of the contract. Coordinate engineering projects and activities into a successful overall Program schedule. Analyze situations and exercise sound judgment in determining appropriate courses of action. Gathering client/user inputs, simplifying complex topics for non-technical audiences and preparing quick painted summaries for executives and stakeholders	Bachelors	5

NOTE: Unless otherwise stated, experience and education may be substituted for each other on a year for year basis.

2.0 TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF CLOUD COMPUTING SERVICES (SPECIAL ITEM NUMBER 518210C)

2.1 SCOPE

The prices, terms and conditions stated under Special Item Number (SIN) 518210C Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this Information Technology Schedule.

This SIN provides ordering activities with access to technical services that run-in cloud environments and meet the NIST Definition of Cloud Computing Essential Characteristics. Services relating to or impinging on cloud that do not meet all NIST essential characteristics should be listed in other SINs.

The scope of this SIN is limited to cloud capabilities provided entirely as a service. Hardware, software and other artifacts supporting the physical construction of a private or other cloud are out of scope for this SIN. Currently, an Ordering Activity can procure the hardware and software needed to build on premise cloud functionality, through combining different services on other IT Schedule 70 SINs (e.g. 54151S).

Sub-categories in scope for this SIN are the three NIST Service Models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Offerors may optionally select a single sub-category that best fits a proposed cloud service offering. Only one sub-category may be selected per each proposed cloud service offering. Offerors may elect to submit multiple cloud service offerings, each with its own single sub-category. The selection of one of three sub-categories does not prevent Offerors from competing for orders under the other two sub-categories.

See service model guidance for advice on sub-category selection.

Sub-category selection within this SIN is optional for any individual cloud service offering, and new cloud computing technologies that do not align with the aforementioned three sub-categories may be included without a sub-category selection so long as they comply with the essential characteristics of cloud computing as outlined by NIST.

See Table 1 for a representation of the scope and sub-categories.
TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF CLOUD COMPUTING SERVICES (SPECIAL ITEM NUMBER 518210C)

Table 1: Cloud Computing Services SIN

SIN Description	Sub-Categories1
• Commercially available cloud computing services • Meets the National Institute for Standards and Technology (NIST) definition of Cloud Computing essential characteristics • Open to all deployment models (private, public, community or hybrid), vendors specify deployment models	1. Software as a Service (SaaS): Consumer uses provider's applications on cloud infrastructure. Does not manage/control platform or infrastructure. Limited application level configuration may be available.
	2. Platform as a Service (PaaS): Consumer deploys applications onto cloud platform service using provider-supplied tools. Has control over deployed applications and some limited platform configuration but does not manage the platform or infrastructure.
	3. Infrastructure as a Service (IaaS): Consumer provisions computing resources. Has control over OS, storage, platform, deployed applications and some limited infrastructure configuration, but does not manage the infrastructure.

2.2 SIN 518210C CLOUD SERVICES

The following Reference documents are available to all customers upon request or in accordance with solicitation instructions.

- Sev1Tech's Response Guidance and Checklist for IT70 Schedule 70 Cloud Sin 518210C
- Sev1Tech's Commercial Pricing Practices
- Sev1Tech's SF30

We recommend all cloud customers read and become familiar with the following NIST and IT70 guidelines.

A. FedBizOpps: IT Schedule 70 Solicitation:
   - Solicitation Attachment 14 - "Critical Information Specific To Schedule 70"
     - This solicitation attachment contains Terms and Conditions for the Cloud SIN, beginning on page 30.
     - Refer to Section 5 (GUIDANCE FOR CONTRACTORS) on page 37 for detailed information and instructions on how to interpret each requirement. This section has been developed for suggestion and guidance only and does not alter NIST definitions or publications.
   - Solicitation Attachment 15 – "Technical Evaluation Criteria SIN 518210C Cloud Computing"
     - This solicitation attachment outlines the technical evaluation criteria for the Cloud SIN.

B. NIST SP 800-145:
   - Definitions of cloud computing, service models and deployment models.

2.2.1 OVERVIEW OF CLOUD SERVICES

The dynamic cloud market with increasing competition and rapid advances in technology provides customers to lower their costs while increasing compute power. Increasing capability, adding flexibility, and improving your security posture are all benefits of cloud managed services with service level commitments. Services can be provided for any FISMA level low through high and in both FedRamp and non-FedRamp environments based on the customers mission requirements. Services per NIST can be provided on premise and or in our network of service providers as complete services. Sev1Cloud minimize IT risks and improves mission availability.

The scope of this SIN is "as a Service" models as defined by NIST. The prices, terms and conditions stated under Special Item Number (SIN) 518210C Cloud Computing Services apply exclusively to Cloud Computing Services within the scope of this Information Technology Schedule and compliant with NIST 800-154 Cloud Computing. Cloud services must be sold in a NIST approved model and bundled into a service fee. Examples: The contractor under SIN 518210C cannot sell a stand-alone sharepoint software licenses and have the government take title of the license. The license must be used as part of a service. The offeror however can define and offer Sharepoint as a Service based on usage specifications. The contractor cannot sell a physical data center or a physical server as that is not part of a service. Offerors must use multiple schedules (54151S) to address these non-cloud service items.

Sev1Tech provides all of the three major types of cloud computing solutions **Infrastructure as a Service (IaaS)**, **Platform as a Service** (PaaS), and **Software as a Service** (SaaS). Although each has its own significance, your choice of the best option may vary depending upon what products or services you're dealing in. Most customers use a variety in their solutions. For example a customer may choose SaaS for email so the do not have to manage it and choose basic IaaS services for a mission application where more control is required.

The foundation for defining services in this market space is NIST. Sev1Tech provides all the NIST 800-145 defined cloud computing services to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service). Customers can choose more than one model as each application has different requirements and advancing from basic service to a complete managed cloud services is part of the service lifecycle. Flexibility to accommodate all mission requirements is essential to this service. Not all customers within even a single organization will leverage the same services or deployment models. Sev1Tech's responsibility as the offeror is to clearly define and document the service model, deployment model, and supporting service level agreements being offered to the customer in all task order responses.

The service models approved by NIST and leveraged by Sev1Tech are as follows:

NIST Defined Service Models	NIST 800-145 Definitions	Benefits To Customers
Infrastructure as a Service (IaaS)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).	Provides application owners the ability to manage this applications and operating systems. This provides a more resilient and flexible environment to operate mission systems.
Platform as a Service (Paas)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.	Provides the customer a managed compute platform that allows resources to focus on the application layers not the operating layers and infrastructure. This model is a great way to improve security compliance and reduce mission availability risk.
Software as a Service (Saas)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).	For customers that want to focus on their mission and not the supporting IT tools this option provides the highest level or service to the end-user.

2.0.2 IaaS, PaaS, and SaaS SERVICE CHARACTERISTICS OVERVIEW:

While Sev1Tech designs custom cloud solutions to your specific requirement, Sev1Tech complies with all NIST guidelines. For specific details for each service please request our Response Guidance and Checklist for IT70 Schedule 70 Cloud Sin 518210C. Below is an overview of how Sev1Tech meets the NIST Service Essential Characteristics.

Sev1Tech's solutions incorporate all of the 5 essential characteristics: On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured services. However customers must clearly define who has on-demand direct access permissions to allocate additional capacity. In some cases, at the Contracting Officers discretion, only the COR may have the authority to add more resources. Adding capacity in the cloud equates to adding cost immediately and cannot be uncommitted.

1. On-Demand Self-Service: In accordance with the customer's deployment and service model requirements and authorization from the contracting officer, Sev1Tech provides on-demand self-service through our web-based customer portals or with direct access to our services. Sev1Tech provides training on incurring additional costs through on-demand access in the cloud as part of our deployment. However, an individual authorized by the CO has the on-demand ability to significantly increase processing and storage costs without any supervision and the customer is obligated to pay for the additional resources at time of commitment.
2. Broad Network Access: Sev1Tech provides multiple methods for connecting to our environments.
   - Clients internet connection

- Dedicated internet connection
- Thin client access
- Open internet access with no access controls
- Single, or dual factor authentication
- Software VPN access to any device, site (building or network) or designated remote/portable users for Microsoft, Linux, Android IoS, Apple, and open source devices.
- Advanced secure internet connections with integrated endpoint management and protection for Microsoft, Linux, Android IoS, Apple, and open source devices
- Software Defined Networking and Common Commercial Carrier services
- Portable hardware encryption keys over internet
- Private dedicated circuit or fiber services with an architected security solution (appliance based)
- Access for IoT devices could be provided via low transmission wireless networks

This allows customers to access the environment for as many locations are they require. This broad access also promotes the capability to connect laptops, workstations, mobile devices, and tablets. For non-web based services in the IaaS, PasS, and SaaS model the customer may choose to leverage private connectivity options to provide additional levels of security controls such as dark fiber.

3. Resource Pooling: Regardless of the service model Sev1Tech can offer resource pooling within the solution. This can be accommodated through cloud brokerage within large platform providers or in private clouds through offerings of virtual machines and shared storage alternatives. We can draw from resource pools across multiple providers and environments if required by the customer. We work with each customer to design a process that ensures we govern elasticity and resource allocation based on their authorization model. The building blocks for our resources are:

Building Blocks Based on Customer Requirements	Standard Measure	Units Offered	Usage Reporting Frequency
Software	Per license used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime
Compute	Per CPU used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime
Storage	Per Gigabyte used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime
Network	Per Megabyte used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime
Facilities Space	Per Rack Unit used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime
Facilities Power	Per KW used or committed	Hourly, Monthly, Yearly	Monthly with Invoice and on-demand self-service or through request anytime

4. Rapid elasticity: Provisioning of compute, storage, and capability using todays technologies are instantaneous. We can design our solutions to meet customer requirements. Sev1Tech provides all the capacity management so you can focus on your mission. Total capabilities far exceed the requirements (example: no one customer can utilize all of AWSs, Azures, or Raging Wires capacity at one time). By using a software define infrastructure and abstracting the physical layers of the solution we auto-scale the environments manage the performance through monitoring wherever possible. We can draw from resource pools across multiple providers and environments if required by the customer. We work with each customer to design a process that ensures we govern elasticity and resource allocation based on their authorization model.

5. Measured Service: Sev1Tech can provide the transparency across our solutions with measured services. We can provide as much detailed information to customers as required. For customer who want solutions were costs float based on daily market demands we can provide metering and cost incurred reporting. For customers who prefer firm fixed price arrangements or buying capabilities in defined year increments we can provide reporting to drive costs down each performance period and offer credits.

2.3 SIN 518210C PRICING

2.3.1 Sev1Tech's CLOUD OPTIMIZATION TRANSPARENT PRICING

With Amazon AWS, Azure, and infrastructure providers changing their technology offering and 100,000s of configuration components on their pricelists every 30-60 days the cloud market remains dynamic and infrastructure is a commodity. With 100,000s of configuration options per provider static pricing becomes very complex and outdated quickly. This is a market driven sector where prices continue to go down and using transparent market time pricing provides additional savings. Sev1Tech always provides the market prices used to calculate our service fees at the time of the task order, not 12 or even 1 month prior. This saves customer money. As your dedicated services broker you can see those costs using the same configurations we do on Amazon, AWS, and other 3rd party providers, every cost is transparent to our customers. For private cloud solutions Sev1Tech provides simple ceiling prices and tailors each solution to your mission requirements.

Sev1Tech makes pricing simple and transparent. Our Cloud Access Fee (CAF) structure helps you buy the right resources at today's market prices. Sev1Tech quotes/purchases the required resources and sets price ceilings based on your required configuration. This allows us to create NIST aligned services based on your security requirements, compute and application service requirements. CAF applies to the infrastructure usage based building blocks and does not apply to labor based support services such as monitoring, SLA support, security, patching, and application support services.

Application of usage based CAF Fees For All Service and Deployment Models		
IaaS	PaaS	SaaS
Facility/Space Usage	Building Blocks Included In Service Costs, Not Labor	Building Blocks Included In Service Costs, Not Labor
Compute Usage		
Storage/Media Usage		
Network Usage		
Appliance Usage		
Building Block Infrastructure Applications: Operating Systems & Middleware		

Sev1Tech always clearly defines and differentiates between core building blocks and support as services are tailored to each customer requirements. We offer flexible cost models that are completely transparent and provided at time of submission. We offer a ceiling price for hourly, monthly and on-demand computing resources but you only pay for what you use. Sev1Tech provides the ability to earn elastic compute credits (ECCs) toward more capacity or compute resource if you don't use all the resources you purchase or we can bill for just what was used, each customer can decide. We optimize your configuration every month to ensure you are using the latest configurations and operating in the cloud at or below your ceiling costs. Examples of CAF savings:

1) Elastic Hourly or Monthly Commitments: A customer orders a medium size server with on demand compute and storage. Sev1Tech charges our CAF to the monthly cost on top of the quoted cost for a specific service configuration. We monitor and optimize your resources reducing usage by 50% of that organizational specified capacity. You then have options to achieve the cost savings:
    a. On a usage based contract for hourly or monthly resources Sev1Tech will only charge you for the actual usage plus CAF saving the customer 40% of the original cost.
    b. On a fixed price contract Sev1Tech can provide an ECCs to use when your application peaks and you need more resources or you can use them to build more capacity for other value added environments like test, development, or Dev-Ops without effecting your budget.
2) Discounted Year Commitments: Some customers leverage 1-year compute commitments to obtain upfront additional discounts for dedicated resources. Carriers discount these instances over hourly on-demand usage. This works well for applications where the processing trends are well known. The customer still pays the current market cost plus the CAF. While the compute is fixed, Sev1Tech still optimizes the storage/media components and other varible costs offering savings or ECCs.
3) On-Premise/Off-Premise Private Services: This deployment model is handled the same way as off premise committed compute environments with maximum ceilings. We will optimize our solution with the best market commodity services. We then evaluate the environment for storage, compute, and application usage

to make recommendations to lower costs quarterly and pass the saving to the customer through price reduction or ECCs.

2.3.2 DISCOUNTS:

While the amount of discount varies by solution, customers can take advantage of the following market discount strategies:

Commitment Discounts Available in the Market:

1) Discounts for 1 year commitments on resources
2) Discounts for 3 year commitments on resources
3) Upgrading to next generation services with more compute and lower cost as they are offered

Sev1Tech offers flexible contracting pricing models aligned with the NIST service delivery and deployment models. We will respond based on the customer's requirements but our two most common are as follows:

1) Fixed Price Ceiling with Elastic Usage Based Pricing: Clients pay only for the services they use on an elastic basis. We provide market estimates directly from the cloud provider and Sev1Tech charges a fixed 10% Cloud Access Fee (CAF) to provide cloud access, optimization of services, building block application and infrastructure components, and consolidated billing. The CAF is applied to all building block cloud service costs which are publicly available through each service on-line cloud configuration managers. Additional services may be added to accommodate NIST service and deployment cloud models (monitoring service, security service, operations support, ect). Any labor requested to support specific IT projects (Migrate a database) are quoted from Sev1Tech's SIN 54151S & SIN 54151HACS SINS.

2) Firm Fixed Price: Clients negotiate a firm solution price for a 1-5 year team. This is best for customers on a set budget that do not want to exceed set costs and know their applications processing patterns well enough to size them correctly. Infrastructure components and application building block services are still subject to the CAF. Additional services may be added to accommodate NIST service and deployment cloud models (monitoring service, security service, operations support, ect). Any task labor requested to support specific IT projects (migrate a database) are modeled from Sev1Tech's 54151S professional services schedule.

2.4 SIN 518210C PRICING MATRIX

SIN	MANUFACTURER NAME	MFR PART NO	PRODUCT NAME	UOI	GSA OFFER PRICE (inclusive of the .75% IFF)
518210C	Sev1Tech	CS-IAAS-009999	IAAS Cloud Services	Monthly	$9,985.85
518210C	Sev1Tech	CS-IAAS-010000	IAAS Cloud Services	Monthly	$99,741.50
518210C	Sev1Tech	CS-IAAS-0100000	IAAS Cloud Services	Monthly	$248,725.57
518210C	Sev1Tech	CS-IAAS-0250000	IAAS Cloud Services	Monthly	$987,349.01
518210C	Sev1Tech	CS-IAAS-10000001	IAAS Cloud Services	Monthly	$1,477,246.88
518210C	Sev1Tech	CS-PAAS-009999	PAAS Cloud Services	Monthly	$9,973.25
518210C	Sev1Tech	CS-PAAS-010000	PAAS Cloud Services	Monthly	$99,489.63
518210C	Sev1Tech	CS-PAAS-0100000	PAAS Cloud Services	Monthly	$248,095.88
518210C	Sev1Tech	CS-PAAS-0250000	PAAS Cloud Services	Monthly	$984,830.27
518210C	Sev1Tech	CS-PAAS-10000001	PAAS Cloud Services	Monthly	$1,473,468.75

SIN	MANUFACTURER NAME	MFR PART NO	PRODUCT NAME	UOI	GSA OFFER PRICE (inclusive of the .75% IFF)
518210C	Sev1Tech	CS-PAAS-009999	PAAS Cloud Services	Monthly	$9,973.25
518210C	Sev1Tech	CS-SAAS-010000	SAAS Cloud Services	Monthly	$99,489.63
518210C	Sev1Tech	CS-SAAS-0100000	SAAS Cloud Services	Monthly	$248,095.88
518210C	Sev1Tech	CS-SAAS-0250000	SAAS Cloud Services	Monthly	$984,830.27
518210C	Sev1Tech	CS-SAAS-10000001	SAAS Cloud Services	Monthly	$1,473,468.75
518210C	Sev1Tech	COF-I-001	IaaS Cloud Optimization Service	Monthly	$0.99
518210C	Sev1Tech	COF-P-001	PaaS Cloud Optimization Service	Monthly	$0.99
518210C	Sev1Tech	COF-S-001	SaaS Cloud Optimization Service	Monthly	$0.99

2.5 SIN 518210C LCAT Rates

LCAT	Year 1	Year 2	Year 3	Year 4	Year 5
Cloud Engineer 5	$218.20	$224.75	$231.49	$238.44	$245.59
Cloud Engineer 4	$152.05	$156.61	$161.31	$166.15	$171.14
Cloud Engineer 3	$130.33	$134.24	$138.27	$142.42	$146.69
Cloud Architect 4	$207.34	$213.56	$219.97	$226.57	$233.37
Cloud Architect 3	$136.80	$140.90	$145.13	$149.48	$153.97
Cloud SME	$192.53	$198.31	$204.26	$210.39	$216.70
Cloud Docker	$119.47	$123.05	$126.75	$130.55	$134.46
Cloud Consultant 4	$130.33	$134.24	$138.27	$142.42	$146.69
Cloud Consultant 3	$112.99	$116.38	$119.87	$123.47	$127.17
Cloud Security Information Analyst	$144.15	$148.48	$152.93	$157.52	$162.25
Cloud Analyst 5	$153.04	$157.63	$162.36	$167.23	$172.25
Cloud Analyst 4	$136.75	$140.85	$145.08	$149.43	$153.91
Cloud Analyst 3	$108.61	$111.87	$115.22	$118.68	$122.24
Cloud Database Engineer	$115.52	$118.99	$122.56	$126.23	$130.02
Cloud Systems Administrator 3	$113.14	$116.53	$120.03	$123.63	$127.34
Cloud Systems Administrator 2	$100.71	$103.73	$106.84	$110.05	$113.35
Cloud Project Manager	$207.34	$213.56	$219.97	$226.57	$233.37
Cloud Solutions Manager	$143.36	$147.66	$152.09	$156.66	$161.36

2.6 SIN 518210C LCAT Descriptions

LCAT	Responsibilities	Experience	Education
Cloud Engineer 5	Researches, designs, develops, runs tests, and evaluates systems that support cloud implementation and integrates with cloud service providers, applying principles and techniques of computer science, engineering, and mathematical analysis.	5	Bachelors
	Plans and conducts technical tasks associated with the implementation and maintenance of internal cloud enterprise-shared virtualization infrastructure.		
	Develops and executes cloud solution roadmaps as they relate to business and executes company strategy to drive the achievement of business objective.		
	Formulates and designs systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.		
	Analyzes cloud requirements to determine feasibility of design within time and cost constraints.		
	Consults with other engineering staff to evaluate interface between hardware and software and operational and performance requirements of overall cloud technology system.		
	Deploys software to cloud computing infrastructure, and works with system configuration and deployment automation technologies, working with ETL tools and techniques.		
	Performs the implementation, operational support, maintenance, and optimization of network hardware, software, and communication links of the cloud infrastructure.		
	Leverages software development and open source solutions to automate tasks required to enable and manage an organization's products and/or services.		
	Resolves complex problems, creates and improves procedures, and facilitates communication.		
	Researches and writes technical documentation that is beneficial to the organization.		
	Provides oversight of hosted systems, databases, and network troubleshooting, and provides various technical solutions to the business.		
Cloud Engineer 4	Ensure a seamless integration between on-premises infrastructure operations and optimal, efficient, and secure consolidated operations for cloud services	3	Bachelors
	Develop and implement a role-based access control strategy integrated with on-premises Active Directory services		
	Manage Cloud providers' applications, infrastructure, and systems		
	Develop, implement, and enforce standard procedures to provision and manage Cloud-based network, storage and infrastructure constructs; standard procedures to provision and manage virtual assets, services, and databases		

LCAT	Responsibilities	Experience	Education
	Ensure resilience, sizing and capacity requirements are met; monitors SLAs and burn rates		
	Professional-level Cloud Certification (Engineer/Architect) minimum		
	Microsoft and or Linux Operating System experience		
	Working knowledge of software development		
	Ability to identify and troubleshoot issues with little oversight		
Cloud Engineer 3	Automate, scale, and patch our multi-region AWS GovCloud cloud infrastructure deployments via CloudFormation, Lambda and Jenkins	2	Bachelors
	Automate application build and deployment pipelines		
	Design new capabilities with best practices and security at the forefront		
	Identify and improve on possible points of failure in the infrastructure/applications		
	Support troubleshooting incidents as they arise and participate in post-mortems		
	Develop documentation and processes to train IT support staff		
	Knowledge of AWS user, security, and networking configurations		
	Familiarity with AWS Services		
	Knowledge of deployment automation tools.		
	Experience scripting in python or bash or comparable language		
	Experience scripting against AWS CLI		
	Familiarity with enterprise CI/CD		
	System Integration and Automation experience preferred		

LCAT	Responsibilities	Experience	Education
Cloud Architect 4	Expert in one or more Azure Cloud Infrastructure (IaaS) offerings and comfortable discussing solutions with clients.	4	Bachelors
	Interfacing with customers to determine technical requirements, feasibility, and expectations.		
	Strategizing with clients to develop solutions based on a variety of criteria including a clear description of services, functionality, scalability, futureproofing, and cost.		
	Designing and communicating compelling solutions that urge prospects to take the desired action.		
	Design Cloud-based solutions using cloud computing architectural procedures that typically consist of front-end platform, back end platforms, cloud-based delivery, and a network.		
	Implement cloud computing architecture solutions that address cloud security and compliance fundamentals, deployment automation and elastic sizing of environments, and multi-tenant implications		
	Design and implement multi-tier architecture solution that is highly available and fault tolerant using Azure platform services		
	Design and implement effective cloud computing solutions that take into account an organization's structure, communications, and operational business processes, including financial management and cost model implications		
	Manage the process of migrating and transitioning to a cloud environment		
	Analyze current workloads, migrate existing IT systems to the cloud, and configure new systems or services to enhance business operations.		
	Manage the implementation of the cloud to ensure a successful deployment.		
	Experience performing requirements gathering with a prospective customer and tailoring a custom product and solution.		
	Experience writing statements of work and appropriately determining pricing and cost.		
	Keen attention to detail, a data-driven critical thinking mind, analytical expertise, and a solution-driven, service-oriented personality.		
	A knack for working in a similar fast-paced, high-SLA, deadline-driven environment.		
	Thorough understanding of Cloud Computing: virtualization technologies, Infrastructure as a Service, Platform as a Service and Software as a Service Cloud delivery models and the current competitive landscape		
	Thorough understanding of infrastructure (firewalls, load balancers, hypervisor, storage, monitoring, security etc.) and have experience with orchestration to develop a cloud solution		
	Programming and scripting experience in programming languages like C#, Python, Java, or JavaScript		

LCAT	Responsibilities	Experience	Education
	Excellent written and verbal communication		
Cloud Architect 3	Provide consultation and strategic guidance to agency IT staff to help shape IT strategy and direction for large, complex agency IT ecosystems. As part of an Enterprise Architecture (EA) program team, develop and maintain key agency EA products to include: Application Life cycle Management (ALM) strategy, continuous integration (CI) and continuous deployment (CD) processes and techniques under an overarching enterprise Platform-as-a-Service, DevOps, and Cloud Strategy. Responsible to build and maintain a CI/CD strategy for the IRS and by extension, the DevOps strategy for application development as well as operations management. Cloud Strategy and Application Rationalization for Cloud Deployment, Cloud Vendor or Platform Selection and Cloud Migration strategy. Build and maintain a cloud infrastructure strategy for federal agencies through providing inputs and advising clients, sometimes by creating the solution architecture or overseeing proofs of concept (POCs), to build multiple software POCs to assess the various needs of the client from the perspective of security, networking, and cloud infrastructure providers. Provide inputs and advise, sometimes by creating a solution architecture or overseeing Proof-of-Concepts (POCs), to build multiple software POCs using the various types of application stack and PaaS solutions, inbuilt or external DevOps tools and methodologies, and come up with an incrementally updated policy, guideline and checklist documents for the enterprise to use. Provide inputs for the new Internal Reference Manuals (IRMs) or rewrite older ones to administer formal approvals for the processes and tools associated with the PaaS and DevOps technologies	2	Bachelors
	The Cloud Architect will work to analyze, design, and architect cloud-based solutions to address customer needs for infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS). Additionally, the Architect partners with both business and technology groups to ensure that the proposed technical solutions and strategy align with and support mission objectives.		
	This role will design, build, and support the long-term strategic roadmap for client IT infrastructure architecture which includes the development and ongoing development and migration to cloud based solutions and the continuous optimization of platform services.		
	Design, build, configure, implement, deliver, and manage Cloud solutions/environments		
	Develop technical architecture and design diagrams and descriptions		
	Use development and scripting tools, language, process, methods, troubleshooting deployment concepts (including continuous integration) and Networking (including Virtual Networks/Virtual Private Cloud, Security Groups, Access Control Lists, CIDR addressing, etc)		
	Support cloud computing services, including IaaS, PaaS, SaaS concepts and articulate concepts to technical and non-technical audiences		

LCAT	Responsibilities	Experience	Education
	Work closely with IT Managers, systems and network engineers, software developers and architects, and third party vendors to deliver robust and scalable infrastructure solutions, improve existing infrastructure capabilities and review and provide recommendations on new technologies		
	Lead the design and modeling of tactical architectures for the delivery, development, and support of projects		
	Develop and maintain policies, standards, and guidelines to ensure that a consistent framework is applied across the organization		
	Analyze existing systems, processes and architectures to make recommendations for improvement		
	Experience in Microsoft Azure or other available cloud services, cloud architecture and components (e.g., compute, storage, backup, network, security, DR, DevOps and IT governance)		
	Working knowledge of supporting IT infrastructure technologies and standards including software & hardware life cycle, system configuration policies, security, hardening, HA, DR etc		
	In depth knowledge on Microsoft core platform technologies based on windows server		
Cloud SME	Provide consultation and strategic guidance to agency IT staff to help shape IT strategy and direction for large, complex agency IT ecosystems. As part of an Enterprise Architecture (EA) program team, develop and maintain key agency EA products to include: Application Life cycle Management (ALM) strategy, continuous integration (CI) and continuous deployment (CD) processes and techniques under an overarching enterprise Platform-as-a-Service, DevOps, and Cloud Strategy. Responsible to build and maintain a CI/CD strategy for the IRS and by extension, the DevOps strategy for application development as well as operations management. Cloud Strategy and Application Rationalization for Cloud Deployment, Cloud Vendor or Platform Selection and Cloud Migration strategy. Build and maintain a cloud infrastructure strategy for federal agencies through providing inputs and advising clients as a subject matter expert (SME), sometimes by creating the solution architecture or overseeing proofs of concept (POCs), to build multiple software POCs to assess the various needs of the client from the perspective of security, networking, and cloud infrastructure providers. Provide inputs and advise as a Subject Matter Expert (SME), sometimes by creating a solution architecture or overseeing Proof-of-Concepts (POCs), to build multiple software POCs using the various types of application stack and PaaS solutions, inbuilt or external DevOps tools and methodologies, and come up with an incrementally updated policy, guideline and checklist documents for the enterprise to use. Provide inputs for the new Internal Reference Manuals (IRMs) or rewrite older ones to administer formal approvals for the processes and tools associated with the PaaS and DevOps technologies.	5	Bachelors
Cloud Docker	The Docker SME will apply their knowledge and experience in assisting Agency to containerize their algorithms and/or applications using tools from the Docker ecosystem in a cloud-based environment. The Docker SME will also be responsible for all aspects of the Docker Container lifecycle in the cloud development environment.	3	Bachelors
	Build Docker Images; maintain Docker Registries; implement Docker networking, Docker security, and Docker storage		

LCAT	Responsibilities	Experience	Education
	Consult with HPC architect and NESDIS scientists to optimize Docker Image for HPC environment		
	Develop wrapper functions for docker calling API for HPC pipelines		
	Monitor, measure, and automate all things to ensure exceed performance and availability goals		
	Participate and potentially lead technical presentations on the work		
	Understand the current systems, algorithms, and cloud based HPC architecture		
	Participate in team meetings and interact with funding clients		
	In-Depth knowledge of Docker Core Ecosystem - Building Docker Images, Registries, Docker networking, Docker storage, Docker security		
	Strong shell scripting skills		
	Strong scripting language skills		
	Ability to use, and build ways to use, automation frameworks		
	Excellent written, oral, and verbal communication skills		
	Experience with IaaS; implementing scalable cloud-based environments and systems; service-oriented architectures and microservices; deploying resilient, scalable, high-throughput systems that process large amounts of data		
Cloud Consultant 4	Designs, develops, implements, utilizes, and conforms to enterprise cloud architecture application solutions, strategies, processes, and standards, focusing on expertise in cloud technologies.	4	Bachelors
	Collaborates with business owners, Analysts, Engineers, development teams, and infrastructure services to define, establish, and communicate application and data architecture standards, policies, and directions.		
	Designs high quality architectures, and drives architecture activities that are aligned to organization requirements set by leadership on behalf of stakeholders and are consistent with enterprise architectural standards.		
	Works closely with Developers to ensure proper implementation, and liaises between the needs of the organization and the Developers.		
	Provides assistance and direction to other cloud teams, ensuring that all technologies work effectively together to improve IT solution cloud performance, and processes change requests.		
	Increases reuse and reduces redundancy in applications and technology designs.		
	Supports the development and updates of enterprise architectural strategies, standards, processes, and tools, as well as the development of strategy, frameworks, best practices, and patterns.		
	Ensures compliance with all architecture directions and standards through cross-organization consulting and direct involvement in development efforts.		

LCAT	Responsibilities	Experience	Education
	Recommends and selects tools for strategic implementation, and monitors adherence to corporate standards in application design, development, and testing.		
	Discovers and defines functional requirements and their relationship to technical requirements; and determines the adequacy of documented requirements for architecture definition for the priorities of the department and organization.		
	Leads teams to foster successful consultations with technical and non-technical project resources to evaluate project scope and program offering opportunities.		
	Conducts analyses and proof-of-concepts for new technologies and solutions.		
	Advises and participates in collaboration sessions with peer groups and business owners to estimate the feasibility of further analysis costs, risks, and opportunities for implementations.		
Cloud Consultant 3	Provides high-level cloud-based specialized technical support and consultation to businesses and IT management.	2	Bachelors
	Collaborates with the development team and Project Managers to deliver infrastructure solutions.		
	Researches and evaluates new cloud-based technological developments and evolving business requirements; analyzes findings and seeks opportunities for improvement.		
	Formalizes recommendations and presents them to IT management for further consideration.		
	Implements cloud infrastructure solution offerings on commercial and government public cloud, private cloud, and hybrid customer environments.		
	Handles complex long-term focused projects involving multiple disciplines or business units.		
	Oversees the development of the technical solution or offering in translating the business needs into technical requirements; identifies gaps, strategic impacts, financial impacts, and the risk profile in the technical solution or offering, and provides technical support.		
	Maintains documentation on existing systems to ensure that changes and optimizations are recorded.		
Cloud Security Information Analyst	The Cloud Security Information Analyst will support the cloud environment software develop life cycle (SDLC) engineering design, development, testing, and implementation complies with DoD Risk Management Framework (RMF) and FedRAMP certification goals as well as provide operational technical analysis and cybersecurity engineering support to the development team. As one of the authorities and subject matter experts (SME) in cybersecurity engineering, leads system design and analysis, will recommend implementing tools and applications to improve cybersecurity capabilities and posture. Leverage industry-based best practices to ensure IA compliance, integration, automation, interoperability and scalability when engineering cybersecurity solutions. In addition to engineering design of major long-term efforts, conducts engineering technical analysis and cybersecurity assessments to resolve complex issues for the development and implementation of operational programs. Will also be responsible for writing	4	Bachelors

LCAT	Responsibilities	Experience	Education
	DoD RMF/FedRAMP plans identified in NIST SP 800-53, such as access control plan, configurations management plans, system security plans, incident response plans, access control, configurations, etc.		
	Conducts cybersecurity engineering by generating recommendations, designing, implementing, and transitioning solutions to improve cybersecurity posture, allow for mission assurance, and comply with all Agency policies.		
	Support system integration, system evaluation and analysis, site surveys, verification and validation, cost and risk, and supportability and effectiveness analyses for total systems and architectures.		
	Conduct advanced research and analysis of current systems to develop strategic implementation plans and designs, document and mitigate risks as well as lessons learned, and provide regular updates.		
	Ensure all requirements, customer and functional, are met though system analysis across all levels to include hardware/software, concept, design, fabrication, test, installation, operation, maintenance and disposal.		
	Support development team to research, collaborate, and strategize with vendors and various groups, such as Systems Security Engineering, R&D, Server and Network teams, and provide recommendations on how to leverage emerging technology to improve cybersecurity and mission assurance.		
	Address unusually complex problems with consultative direction through the application of advanced cyber security technologies expertise, security principles, theories, and concepts.		
	Maintain a strong understanding of cybersecurity, networking architecture, servers, systems design, virtual hosts, and configuration management and licensing.		
	Provide expertise to contribute to the security assessment and compliance activities to maintain accreditation to include mitigation and documentation.		
	Analyze and research vulnerabilities to identify risk to provide early warning related to a variety of cyber threats.		
	CAP or SSCP Certification		
	Experience with cyber security software System Development Life Cycle		

LCAT	Responsibilities	Experience	Education
	Strong experience with cloud security strategy, cloud provider ecosystems (AWS) infrastructure, application and data designs to hybrid or fully cloud enabled practices.		
	Advanced cybersecurity systems engineering design and operations in multi-enclave cloud environments.		
	Possess clear understanding of security protocols and standards and have experience with software security architectures.		
Cloud Analyst 5	Will have substantial experience providing cloud infrastructure baselining and opportunity assessment support, as well as developing sequenced migration plans for infrastructure, services, and data.	3	Bachelors
	Work with Enterprise Platforms Lead and Cloud Readiness Team to support the development of cloud migration inputs and solutions, from needs analysis and environment baselining and assessment, through the development of a detailed phased cloud migration plan/roadmap.		
	Evaluate architectural frameworks/patterns, processes, standards, and guidelines related to cloud, enterprise, and data architecture, and align cloud approach with overall enterprise architecture vision.		
	Support cloud readiness and feasibility assessments, workshops, roadmap, and application modernization discussions.		
	Assess, provide recommendations, and develop implementation plans for cloud migration, operation, and optimization.		
	Provide technical expertise in resolving challenging technical problems, and in identifying risks with associated mitigations.		
	Create a playbook for identifying, assessing, and prioritizing enterprise applications, systems, and data for migration to the cloud. The playbook shall incorporate established technical criteria, migration drivers, and technical/organizational constraints.		
	Functional knowledge of cloud technologies (IaaS, PaaS, SaaS).		
	Experience defining, designing and/or implementing cloud solutions		
	Familiarity with Software Development Life Cycle (SDLC) or similar methodologies.		
	Experience gathering requirements and capturing user stories.		
	Familiarity with business analyses, including gap analysis, process mapping, root-cause analysis, and risk analysis.		
	AWS, Azure, or similar Cloud certification or experience.		
	Excellent communication skills: verbal, written, and presentation.		
	Facility communicating with and managing stakeholders across all organizational levels.		
Cloud Analyst 4	Analyzes cloud-related business requirements and project objectives, and develops application functional specifications.	2	Bachelors
	Analyzes computer input, designs complex data sets, and envisions the data.		

LCAT	Responsibilities	Experience	Education
	Researches and develops original solutions to help client solve big data problems and to build holistic solutions for the client, to help save time, money, and resources.		
	Communicates with technical and non-technical users, business stakeholders or clients, developers, end-users, and Project Managers.		
	Gathers and evaluates project requirements, meets with customers and partners to outline expectations, and defines stakeholder alignment.		
	Discusses best practices for cloud for sales, service, and social projects across multiple methodologies.		
	Keeps up to date on current and road-mapped cloud features, functionality, and terminology.		
	Manages follow-ups and action items from meetings with Consultants, Service Delivery Managers, and/or Account Managers.		
	Serves as a functional advisor and problem solver to stakeholders to assist them in understanding and optimizing data and their use of the product to define, build, and deploy online applications.		
	Researches new developments.		
	Writes advanced analytics on cloud-based technologies, serves as a subject matter expert for updating and automating traditional analytical techniques through cloud-based solutions or automation and scripting.		
Cloud Analyst 3	Cloud Analyst 1 is responsible for planning and engineering of an organization's cloud computing infrastructure and applications. Implements and designs hardware and software. Being a Cloud Systems Analyst monitors the performance of systems. Additionally, Cloud Systems Analyst is familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS). Typically reports to a supervisor or manager. Gains exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.	1	Associates
Cloud Database Engineer	Provides technical expertise for database design, development, implementation, information storage and retrieval, data flow and analysis	3	Bachelors
	Develops relational and/or Object-Oriented databases, database parser software, and database loading software		
	Projects long-range requirements for database administration and design		
	Responsible for developing a database structure that fits into the overall architecture of the system under development and has to make trades among data volumes, number of users, logical and physical distribution, response times, retention rules, security and domain controls		
	The DBE works primarily at the front end of the lifecycle-requirements through system acceptance testing and Initial Operational Capability (IOC)		
	Develops requirements from a project's inception to its conclusion for a particular business and IT subject matter area (i.e., simple to complex systems)		

LCAT	Responsibilities	Experience	Education
	Assist with recommendations for, and analysis and evaluation of systems improvements, optimization, development, and/or maintenance efforts		
	Translates a set of requirements and data into a usable document by creating or recreating ad hoc queries, scripts, and macros; updates existing queries, creates new ones to manipulate data into a master file; and builds complex systems using queries, tables		
Cloud Systems Administrator 3	Administers, develops, configures, implements, and maintains the systems that comprise the underlying cloud platform.	4	Bachelors
	Sets up public and/or private cloud systems, understanding and depending on type of workload, and deploys them in an automated way; and monitors, moves, and alters the systems using a prescribed methodology.		
	Establishes and implements standards for cloud operations according to specifications and parameters.		
	Determines business needs, and selects a cloud provider(s) that best fits the requirements.		
	Questions and determines cost, business use, location of users, security, and other vectors, which brings the position closer to the business and its goals.		
	Troubleshoots when problems arise, and plans for future cloud capacity requirements.		
	Coordinates and works with others on various parts of the implementation.		
	Schedules, performs, and monitors system backups and, when necessary, performs data recoveries.		
	Recommends upgrades according to growth statistics and forecasts.		
	Schedules, plans, and performs system upgrades, including coordinating the transition from test to production environments.		
	Provides technical support for system users.		
Cloud Systems Administrator 2	Systems Administrator maintains and supports the integrity of the operating system environment and various computer systems. Administers, installs and troubleshoots a variety of operating systems. Being a Systems Administrator II performs systems maintenance tasks, such as system back-up, recovery and file maintenance. Schedules, installs, and tests system software upgrades. Additionally, Systems Administrator configures software and resolves technical problems. Monitors and maintains software licensing and maintenance agreements. Typically reports to a project leader or manager. The Systems Administrator II gains exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.	1	
Cloud Project Manager	Conducts financial and budgetary analysis to define project worth and to ascertain which system best fits user needs and company standards.	4	Bachelors
	Selects project team members and assigns tasks and responsibilities.		

LCAT	Responsibilities	Experience	Education
	Provides direction and technical guidance to project team members; communicates job expectations; and plans, monitors, and appraises job results.		
	Plans, initiates, coordinates, and enforces systems, policies, and procedures.		
	Manages, coordinates, and establishes priorities for complete life-cycle of projects including the planning, design, programming, testing, and implementation of business solutions designed to meet requirements of various departments in the company, such as distribution, finance, and manufacturing.		
	Designs project plans, which identify needs and define major tasks and milestones, based on scope, resources, budget, and personnel.		
	Determines project needs and acquires resources required for the success of the project.		
	Coordinates the development of new systems and/or applications projects, the modification of existing systems or applications, or changes in current methods or techniques.		
	Coordinates project performance with the other work of the affected department or departments.		
	Excludes those who do not have full-time responsibility for project management.		
	Performs feasibility studies to ensure systems adhere to standards and meet user requirements.		
	Conducts financial and budgetary analysis to define project worth and to ascertain which system best fits user needs and company standards.		
	Selects project team members and assigns tasks and responsibilities.		
	Provides direction and technical guidance to project team members.		
	Acts as liaison between implementation personnel, management, and vendors by conducting meetings to review project details and obtain approval and signoffs.		
	Diagnoses and corrects system problems with help from vendors and support team.		
	Oversees production of all deliverables and assesses and enforces project deadlines and works within budget restraints.		
	Processes working knowledge of technical resources such as operating systems, programming languages, and hardware.		
	Manages the agreed scope of the organization's cloud solution projects, and provides innovative solutions to complex problems for the purpose of increasing the speed of development and change and of driving the achievement of business objectives.	4	Bachelors

LCAT	Responsibilities	Experience	Education
Cloud Solutions Manager	Oversees the development of cloud solution roadmaps of the overall vision that underlies the projected solution, transforms that vision through execution into the solution, and assures projects meet the quality requirements.		
	Coordinates solution planning for cloud-based offerings, heads a cloud solution team required to support the business sales channels, and executes the cloud strategy as a leader within the business, utilizing strong technical leadership and ongoing coaching of direct reports.		
	Manages and heads the development and implementation of cloud-based initiatives to ensure that systems are scalable, reliable, secure, and supportable and that they achieve business and IT performance and budgetary objectives.		
	Determines the overall project plan, budget, structure, schedule, and staffing requirements for complex cloud solutions, and collaborates and manages the resources across multiple projects to ensure scheduled delivery of solutions.		
	Shares and communicates ideas clearly, both orally and in writing, to executive staff, business sponsors, and technical resources in clear concise language that is the appropriate for each group.		
	Hires, trains, and develops new Cloud Solutions Architects and other solutions staff from internal and external sources.		

3.0 TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBER SECURITY SERVICES (HACS) (SPECIAL ITEM NUMBERS 54151HACS)

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

3.1 SCOPE

a. The labor categories, prices, terms and conditions stated under Special Item Numbers 54151HACSA, 54151HACSB, 54151HACSC and 54151HACSD 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.
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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 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.

3.9 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.

3.10 RESUMES

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

3.11 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.

3.12 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 54151HACS 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 and minimum education. Unless otherwise stated, experience and education may be substituted for each other on a year for year basis.

Labor Category	PRICE OFFERED TO GSA (including IFF)
Cyber Security Engineer 1	$ 117.27
Cyber Security Engineer 2	$ 134.86
Cyber Security Engineer 3	$ 146.59
Cyber Security Engineer 4	$ 148.55
Cyber Security Engineer 5	$ 189.35
Information Security Consultant 1	$ 136.82
Information Security Consultant 2	$ 146.59
Information Security Consultant 3	$ 161.25
Information Security Consultant 4	$ 214.02
Information Security Consultant 5	$ 242.36
Information Security Manager	$ 180.80
Cyber SME V	$ 148.10
Cyber SME VI	$ 166.37

3.12.1 DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

CLIN	Labor Category Title	Functional Responsibilities	Minimum Education	Minimum Experience
1	**Cyber Security Engineer 1**	The Cyber Security Engineer I may identify or resolve highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to continue as normal. The Cyber Security Engineer is capable of providing discovery of penetration testing artifacts, response to cyber security incidents, operate the tools required for cyber hunt activities and provide fact finding in regards to Risk and Vulnerability assessments. Additionally, The Cyber Security Engineer designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Performs more routine cyber security aspects of the position and is supervised by a higher level of Engineer for additional insights and guidance to perform the necessary support requirements.	**BS**	**1**
2	**Cyber Security Engineer 2**	The Cyber Security Engineer II may identify or resolve highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to continue as normal. The Cyber Security Engineer is capable of providing detailed discovery of penetration testing artifacts and target nodes, response to cyber security incidents and provide contribution to resolution, install/operate the tools required for cyber hunt activities and provide detailed fact finding in regards to Risk and Vulnerability assessments. Additionally, The Cyber Security Engineer designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to incidents, investigates violations, and recommends enhancements to plug potential security gaps. Performs routine cyber security aspects of the position along with experience to address 0 day cyber threats and is supervised by a higher level of Engineer for additional insights and guidance to perform the necessary support requirements.	**BS**	**3**
3	**Cyber Security Engineer 3**	The Cyber Security Engineer III identifies or resolve highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to continue as normal. The Cyber Security Engineer is capable of providing analysis of penetration testing artifacts and target nodes, response to cyber security incidents and provide resolution, install/operate/configure the tools required for cyber hunt activities and provide detailed fact finding in regards to Risk and Vulnerability assessments. The Cyber Security Engineer designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to priority incidents, investigates priority violations, and recommends enhancements to plug potential security gaps in compliance. Provides guidance to Cyber Security Engineer's I & II as to the aspects of cyber security to address cyber threats and provides supervision support to a higher level of Engineer for insights and guidance as it relates to Cyber Security.	**BS**	**5**

CLIN	Labor Category Title	Functional Responsibilities	Minimum Education	Minimum Experience
4	**Cyber Security Engineer 4**	The Cyber Security Engineer IV identifies or resolve highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to continue as normal. The Cyber Security Engineer will be capable of providing detailed analysis of penetration testing artifacts and target nodes, response to escalated cyber security incidents and provide resolution, install/operate/configure the tools required for cyber hunt activities and provides detailed information in regards to Risk and Vulnerability assessments. Delivers consultative analysis directly to a customer as to findings, violations or remediation efforts. The Cyber Security Engineer designs, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to priority incidents, investigates priority violations, and recommends enhancements to eliminate potential security gaps in compliance. The Cyber Security Engineer is considered experienced in the field of Penetration Testing, Incident Response, Cyber Hunt and Risk and Vulnerability assessments. Provides guidance to Cyber Security Engineer III's as to the aspects of cyber security to address cyber threats and provides supervision support to a higher level of Engineer for insights and guidance as it relates to Cyber Security. Performs more varied and difficult tasks which were escalated from level I through III Cyber Security Engineers.	**BS**	**7**
5	**Cyber Security Engineer 5**	The Cyber Security Engineer V provides leadership throughout the identification and resolution of highly complex issues to prevent cyberattacks on information systems or keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, or theft of sensitive customer data, allowing business to operate as normal. The Cyber Security Engineer will be capable of providing detailed analysis of penetration testing artifacts and target nodes, response to escalated cyber security incidents and provide resolution, analyze the outputs from tools required for cyber hunt activities and provides detailed information in regards to Risk and Vulnerability assessments. Delivers consultative analysis directly to a customer as to findings, violations or remediation efforts. The Cyber Security Engineer sets forth design strategies, installs, and manages security mechanisms that protect networks and information systems against hackers, breaches, viruses, and spyware. This individual responds to priority incidents, investigates priority violations, and recommends enhancements to eliminate potential security gaps in compliance. The Cyber Security Engineer is considered senior in the field of Penetration Testing, Incident Response, Cyber Hunt and Risk and Vulnerability assessments. Creates strategy and sets forth plans to provide secure solutions and is highly competent in the subject matter and concepts and may lead individuals assisting in the work. Provides leadership to Cyber Security Engineer I-IV as to the aspects of cyber security to address cyber threats and provides supervision support and guidance as it relates to Cyber Security.	**MS**	**9**
6	**Information Security Consultant 1**	Completes tasks designed to ensure security of the organization's systems and information assets. Protects against unauthorized access, modification, or destruction of data through the use of penetration testing and risk and vulnerability assessment guidance. Has the ability to recommend incident response actions and Cyber Hunt activities based on knowledge of the system and detected activities. Works with end users to determine needs of individual departments. Implements policies or procedures and tracks compliance throughout the organization. Typically requires a bachelor's degree or its equivalent. Typically reports to a manager. Works on projects/matters of limited complexity in a support role. Work is closely managed.	**BS**	**2**
7	**Information Security Consultant 2**	Completes tasks designed to ensure security of the organization's systems and information assets. Protects against unauthorized access, modification, or destruction and develops IT security policies and standards that align to penetration testing and risk and vulnerability assessment best practices as defined within DoD and other government standards. Capable of developing Incident response plans and Cyber Hunt Hypothesis'. Works with end users to determine needs of individual departments. Implements policies or procedures and tracks compliance throughout the organization. Typically requires a bachelor's degree or its equivalent. Typically reports to a manager. Gaining exposure to some of the complex tasks within the job function. Occasionally directed in several aspects of the work.	**BS**	**4**

CLIN	Labor Category Title	Functional Responsibilities	Minimum Education	Minimum Experience
8	**Information Security Consultant 3**	Completes tasks designed to ensure security of the organization's systems and information assets. Protects against unauthorized access, modification, or destruction and develops IT security policies and standards. Works with end users to determine needs of individual departments. Understands internet architecture and firewall configuration to protect system security. May need to authorize user access and familiar with domain structures and digital signatures. Capable of making detailed architectural and configuration recommendations based on penetration testing and risk and vulnerability assessment testing of system infrastructure. Capable of recommending security tool configurations to align with system architecture for increased cyber hunt capabilities and incident response. Requires a bachelor's degree or its equivalent. Typically reports to a manager. Contributes to moderately complex aspects of a project. Work is generally independent and collaborative in nature.	**BS**	**6**
9	**Information Security Consultant 4**	Designs and implements information security standards for applications and databases bases on penetration testing and risk and vulnerability assessment activities. Collaborates with a team of information security analysts to provide subject matter expertise on application development, database design, network maintenance, incident response, and cyber hunt. Researches and advocates the latest technologies and solutions to support the security requirements of internal and external customers and is capable of performing penetration testing and risk and vulnerability assessments of latest technologies. Assesses client needs against security concerns and resolves information security risk issues based on assessment findings. Provides the customer with a detailed understanding of how new technologies will integrate into current Cyber Hunt and Incident response activities. Trains security awareness to business partners and IT staff. Requires a bachelor's degree or its equivalent. Typically reports to a manager. A specialist on complex technical and business matters. Work is highly independent. May assume a team lead role for the work group.	**MS**	**8**