U.S. General Services Administration

MAS
Federal Supply Service
Authorized Federal Supply Schedule Price List
On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order are available through GSA Advantage!®, a menu-driven database system. The INTERNET address GSA Advantage!® is: GSAAdvantage.gov.

SPECIAL ITEM NUMBER 54151HACS – Highly Adaptive Cybersecurity Services (HACS)
SPECIAL ITEM NUMBER 518210C – Cloud and Cloud Related IT Professional Services
SPECIAL ITEM NUMBER 54151HEAL- Healthcare Informational Technology

SPECIAL ITEM NUMBER 54151S- InformationTechnology (IT) Services

FPDS Code D301 IT Facility Operation and Maintenance
FPDS Code D302 IT Systems Development Services
FPDS Code D306 IT Systems Analysis Services
FPDS Code D307 Automated Information Systems Design and Integration Services
FPDS Code D308 Programming Services
FPDS Code D310 IT Backup and Security Services
FPDS Code D311 IT Data Conversion Services
FPDS Code D313 Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) Services
FPDS Code D316 IT Network Management Services
FPDS Code D317 Creation/Retrieval of IT Related Automated News Services, Data Services, or Other Information Services (All other information services belong under Schedule 76)
FPDS Code D399 Other Information Technology Services, Not Elsewhere Classified

z SofTech Solutions, INC
235 Peachtree Street, Suite 400
Atlanta, GA 30303
www.zsoftechsolutions.com
678-778-7817

Contract Number: 47QTCA20D005K
Period Covered by Contract: January 31, 2020 through January 30, 2025

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

Contract period
Note 1: All non-professional labor categories must be incidental to and used solely to support hardware, software, and/or professional services, and cannot be purchased separately.

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

Note 3: This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration, or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

Customer Information:

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

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud and Cloud Related IT Professional Services</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare Information Technology (HIT)</td>
</tr>
<tr>
<td>54151S</td>
<td>- Information Technology (IT) Services</td>
</tr>
</tbody>
</table>

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.
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.

2. Maximum Order: $500,000.00

3. Minimum Order: $100.00

4. Geographic Coverage (delivery Area): Domestic (50 States, DC, PR) & Overseas

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

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

7. Quantity discounts: None offered

8. Prompt payment terms: Net 30 days

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

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

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

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

11b. Expedited Delivery. The Contractor will insert the sentence “Items available for expedited delivery are noted in this
price list.” under this heading. The Contractor may use a symbol of its choosing to highlight items in its price list that
have expedited delivery: Contact Contractor

11c. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also,
the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day
delivery: Contact Contractor

11d. Urgent Requirements. The Contractor will note in its price list the “Urgent Requirements” clause of its contract and
advise agencies that they can also contact the Contractor’s representative to effect a faster delivery: Contact Contractor

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

13a. Ordering Address(es):
Z SofTech Solutions, INC
235 Peachtree Street, Suite 400
Atlanta, GA 30303
www.zsoftechsolutions.com
678-778-7817
13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs), and a sample BPA can be found at the GSA/FSS Schedule homepage (fss.gsa.gov/schedules).

14. Payment address(es):
Z SofTech Solutions, INC
235 Peachtree Street, Suite 400
Atlanta, GA 30303
www.zsoftechsolutions.com
678-778-7817

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

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

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

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

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

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

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

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

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

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

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

24b. If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g. contactor’s website or other location.) The EIT standards can be found at: www.Section508.gov/.

25. Data Universal Numbering System (DUNS) number: 079434552 and CAGE CODE:78H69

26. Notification regarding registration in the System for Award Management (SAM) Database: Registered
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SIN 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-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
1. SCOPE
a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.

b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on MAS and may be quoted along with services to provide a total solution.

c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.

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

e. SCOPE:

54151HACS Highly Adaptive Cybersecurity Services (HACS) - SUBJECT TO COOPERATIVE PURCHASING includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture.

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

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

The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing. HACS vendors are able to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

Sub-Categories - (not all vendors have been placed within the following subcategories. To view a complete list of vendors, click on the SIN)

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

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

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

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

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

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

2. ORDER

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

3. PERFORMANCE OF SERVICES
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
   b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
   c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
   d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor’s travel.

4. INSPECTION OF SERVICES
   Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS COMMERCIAL ITEMS (Jan 2017) & (ALTERNATE I-Jan 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR
   Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (May 2014) Rights in Data – General, may apply.
   The Contractor shall comply with contract clause (52.204-21) to the Federal Acquisition Regulation (FAR) for the basic safeguarding of contractor information systems that process, store, or transmit Federal data received by the contract in performance of the contract. This includes contract documents and all information generated in the performance of the contract.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY
   Subject to the ordering activity security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Highly Adaptive Cybersecurity Services.

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST
   a. Definitions.
   “Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
   “Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
   An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.
   b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations
related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

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

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

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

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING
Please refer to the labor category descriptions and pricing incorporated into this GSA Pricelist.

LABOR CATEGORY DESCRIPTIONS:
HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) SIN 54151HACS

Testing and Validation Specialist Cybersecurity-
Functional Responsibility: Cybersecurity subject matter specialist providing test and evaluation plans for the support of user requirements of complex to highly complex software/hardware applications. Directs and/or participates in all phases of risk management assessments, vulnerability scans and software/hardware development with emphasis on identifying security issues based on vulnerabilities and/or data configuration. May conduct and support authorized penetration testing on enterprise network assets. Suggest security controls in order to mitigate risk.
Educational Requirements: Bachelor’s Degree in Computer Science, Computer Information Systems, or Engineering Experience:
Minimum / General - 5 Years’ Experience

Security Operations Center (SOC) Analyst 1
Minimum/General Experience: 0
Functional Responsibility: Provide cyber threat analysis and reporting to support SOC and Program’s situational awareness. Actively monitor security threats and risks. Track investigation results and report on findings. Duties may include: support Security Operations Center and monitors security tools to review and analyze pre-defined events indicative of incidents and provide first tier response to security incidents; follow standard operating procedures for detecting, classifying, and reporting incidents under the supervision of Tier 2 and Tier 3 staff; and, managing cases within incident management systems.
Minimum Education: Bachelor’s Degree

Risk and Vulnerability Threat Analyst 1
Minimum/General Experience: 2
Functional Responsibility: Participate in conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: provides technical support on post event network security logs and trend analysis; uncovers security and compliance violations; associates and correlates IP address related events with
specific systems or devices in the IT infrastructure; support development and analysis of system and security documentation; maintain documentation for exceptions to standards.
Minimum Education: Bachelor’s Degree

**Incident Response Analyst 1**
Minimum/General Experience: 2
Functional Responsibility: Contributes to generating response to crisis or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: handle and respond to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices; intake incident reporting, conduct ticket updates, and notify stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinate response to computer security incidents; recommend a course of action on each incident and creates, manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally; establishes alarm/incident escalation process and tracks, follows-up, and resolves incidents; and, initiates and maintains contact with affected parties during incident response lifecycle.
Investigates potential incidents/intrusions.
Minimum Education: Bachelor’s Degree

**Cyber Technical Architect 1**
Minimum/General Experience: 2
Functional Responsibility: The Cyber Technical Architect 1 provides thought leadership related to current and future customer plans with regard to protecting customer information technology from cyber threats. This individual possesses knowledge of the future direction and trends associated with the stated information technology, and is up to date with current threats associated with it. This individual is experienced in designing and implementing protections for information architecture solutions for the stated information technology. This individual designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.
Minimum Education: Bachelor’s Degree

**Cyber Security Analyst I**
Minimum/General Experience: 2
Functional Responsibility: Cyber Security Analyst I will have a basic understandings of concepts and terms related access control systems; cryptography; security architecture; operations security; applications security and systems development; statutory and regulatory compliance; forensics, investigations, or security ethics. The Cyber Security Analyst I will assist in penetration testing, incident response and cyber hunt activities as well as systems certification and accreditation projects, including the development of system documentation, system hardening, safeguard implementation, vulnerability assessments, and risk analysis. They will assist with the management and administration of enterprise security programs.
Minimum Education: Bachelor’s Degree

**Cyber Security Engineer I**
Minimum/General Experience: 2
Functional Responsibility: Participate in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serve as a point of contact for engineering efforts while assisting in
maintaining compliance with the customer's policies and guidelines. Duties may include: provide administrative support to enterprise security devices; provide support of various applications and implement security standards; and, assist with configuration, validate secure complex systems, and test security products and systems to detect security weakness. Cyber Security Engineer I develops cyber security systems assurance programs and control guidelines. Capable of performing vulnerability scans of networks, providing technical evaluations, identifying risks and proposing mitigation strategies, conducting system-specific tests and evaluations in realistic network configurations to validate secure operational capabilities and/or discover vulnerabilities, performing residual risk analysis to support system assessment and authorization.

**Minimum Education:** Bachelor’s Degree

**Security Operations Center (SOC) Analyst 2**

Minimum/General Experience: 2

Functional Responsibility: Provide cyber threat analysis and reporting to support SOC and Program’s situational awareness. Actively monitor security threats and risks. Track investigation results and report on findings. Duties may include: support Security Operations Center and monitors security tools to review and analyze pre-defined events indicative of incidents and provides first tier response to security incidents; monitor network traffic for security events and perform triage analysis to identify security incidents; respond to computer security incidents by collecting, analyzing, preserving digital evidence and ensure that incidents are recorded and tracked in accordance with SOC requirements; work closely with the other teams to assess risk and provide recommendations for improving our security posture; recommend content to detect security events; managing cases within incident management systems; perform network Forensics and deep packet analysis; and, identify countermeasures to detect and prevent security incidents.

**Minimum Education:** Bachelor’s Degree

**Cyber Security Specialist 1**

Minimum/General Experience: 2

Functional Responsibility: The Cyber Security Specialist 1 may identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist 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. Level 1 performs more routine aspects of the position and is supervised by higher levels.

**Minimum Education:** Bachelor’s Degree

**Cyber Application Architect 1**

Minimum/General Experience: 2

Functional Responsibility: The Cyber Application Architect may plan, design, develop, redesign or enhance, install, or implement various cyber technology products, or enhance computer programs. This individual applies knowledge of software and programming to develop and test the security of computer systems and produce the necessary outcome for clients. The Application Architect may draft technical white papers to better understand the cyber technology behind them, and to provide instructions that help the client better understand the nature and applications of a specific cyber product.

**Minimum Education:** Bachelor’s Degree
**Risk and Vulnerability Threat Analyst 2 -**
Minimum/General Experience: 4
Functional Responsibility: Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: develop, document and execute containment strategies; document and brief the business on remediation options and execute the plan with stakeholders; produce final report and recommendation; coordinate efforts of, and provide timely updates to, multiple business units during response; performing in-depth analysis in support of incident response operations; develop requirements for technical capabilities for cyber incident management; investigate major breaches of security and recommending appropriate control improvements; work with infrastructure and application support teams to drive closure of follow up actions identified through incident and problem management; performs Security Control Assessments on systems to validate the results of risk assessments and ensure controls in the security plan are present and operating correctly on the system; provides thorough report of the risks to the system and its data; and, develop and analyze system and security documentation. Minimum Education: Bachelor’s Degree

**Incident Response Analyst 2 -**
Minimum/General Experience: 4
Functional Responsibility: Contributes to generating responses to crisis or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: provides oversight for incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets; performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malecode prevention, Firewalls, IDS & IPS, Web security, anti-spam, etc; performs the role of Incident Coordinator for IT Security events requiring focused response, containment, investigation, and remediation; performs forensic analysis on hosts supporting investigations; and, conducts malware analysis in out-of-band environment (static and dynamic), including complex malware. Minimum Education: Bachelor’s Degree

**Cyber Program Analyst -**
Minimum/General Experience: 4
Functional Responsibility: The Cyber Program Analyst analyzes and critiques existing computer programs and systems security measures, and develops new measures. The program analyst may: review users’ requests for new or modified computer programs to determine feasibility, cost and time required, compatibility with current system, and security capabilities; outline steps required to develop program, using structured security analysis and design; and, plan, develop, test, and document computer programs, applying knowledge of cyber security, programming techniques, and computer systems. Minimum Education: Bachelor’s Degree

**Cyber Security Analyst II**
Minimum/General Experience: 4
Functional Responsibility: Cyber Security Analyst II supports development of technical solutions to support client’s requirements in solving moderately complex network, platform, and system security problems. They will assist with the management and administration of enterprise security programs. Responsibilities include: assisting with incident
response, cyber hunt activities, penetration testing, cyber system engineering, development, and monitoring. Cyber Security Analyst II will also conduct security control assessments with cyber security stakeholders, collect and review artifacts and evidence for compliance with security controls, and document assessment results in a security assessment report and risk assessment report.

Minimum Education: Bachelor’s Degree

**Security Operations Center (SOC) Analyst 3 -**

Minimum/General Experience: 4

Functional Responsibility: Provide cyber threat analysis and reporting to support SOC and Program’s situational awareness. Actively monitor security threats and risks. Track investigation results and report on findings. Duties may include: support a Security Operations Center and monitors security tools to review and analyze pre-defined events indicative of incidents and provide first tier response to security incidents; lead shifts and functional IR teams, provides oversight and be responsible for event investigation and tracking activities; support Tier 2 operations by monitoring alerts during critical and high volume events; conduct more in-depth analyses of security incidents to identify incidents of compromise; perform intrusion scope and root cause analyses and assist with intrusion remediation, strategy development, and implementation; recommend effective process changes to enhance defense and response procedures; use SOC monitoring devices to review and analyze pre-defined events indicative of incidents, create and recommend content to detect security events; conduct malware analysis in out-of-band environment (static and dynamic), including complex malware; vet IOCs and intelligence vetting and disposition, assess feed viability; perform network Forensics and deep packet analysis; identify countermeasures to detect and prevent security incidents.; and, support knowledge management and developing procedures and policies for initial stand up of a security operations center (SOC).

Minimum Education: Bachelor's Degree

**Cyber Security Specialist 2 -**

Minimum/General Experience: 4

Functional Responsibility: The Cyber Security Specialist 2 may identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist 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. Level 2 performs more varied and difficult tasks compared to Level 1, yet has less autonomy than Level 3.

Minimum Education: Bachelor’s Degree

**Cyber Security Engineer II -**

Minimum/General Experience: 4

Functional Responsibility: Participate in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serve as a point of contact for engineering efforts while maintaining compliance with the customer's policies and guidelines. Duties may include: configure and maintain policies; maintain documentation for exceptions to standards; provides timely and adequate response to threats/alerts; assess security events to drive to a resolution; provides timely and sufficient response to security incidents and assessment services; and, promotes security awareness. Cyber Security Engineer II develops cyber security systems assurance programs and control guidelines. Capable of performing vulnerability scans of networks, providing technical evaluations, identifying
risks and proposing mitigation strategies, conducting system-specific tests and evaluations in realistic network configurations to validate secure operational capabilities and/or discover vulnerabilities, performing residual risk analyses to support system certification and accreditation. Insures that solutions are fully compatible with or engineered into the customer’s network design.

Minimum Education: Bachelor’s Degree

**Cyber Application Systems Analyst -**
Minimum/General Experience: 2

Functional Responsibility: The Cyber Application System Analyst may oversee the implementation of required hardware and software security components for approved applications, coordinates security tests of the application system to ensure proper performance, and develops diagrams and flowcharts for computer programmers to follow. This individual previews, analyzes, and modifies programming systems, including encoding, debugging, and installing security measures to support an organization's application systems. The Cyber Application System Analyst develops application specifications, identifies the required inputs, and formats the output to meet user's needs.

Minimum Education: Bachelor’s Degree

**Cyber Operations Manager -**
Minimum/General Experience: 4

Functional Responsibility: The Cyber Operation Manager manages, coordinates, or organizes department cyber operation strategies and activities. The Operation Manager may: collaborate in the development and implementation of organization cyber policies, practices, procedures, and attainment of operating goals; review, analyze, and prepare reports, records, and directives, and confers with managers/supervisors to obtain data required for planning activities, such as new commitments, status of work in progress, and problems encountered; and, disseminate policies and objectives to supervisors/staff.

Minimum Education: Bachelor’s Degree

**Cyber Technical Architect 2 -**
Minimum/General Experience: 4

Functional Responsibility: The Cyber Technical Architect 2 provides thought leadership related to current and future customer plans with regard to protecting customer information technology from cyber threats. This individual possesses knowledge of the future direction and trends associated with the stated information technology, and is up to date with current threats associated with it. This individual has experience in designing and implementing protections for information architecture. This individual designs secure architecture to include the software, hardware, and communications to support the total requirements as well as provide for present and future cross-functional requirements and interfaces.

Minimum Education: Bachelor’s Degree

**Risk and Vulnerability Threat Analyst 3**
Minimum/General Experience: 8

Functional Responsibility: Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: support engineering design teams by assessing network and system security design features and making recommendations concerning overall security accreditation readiness and compliance and best practices; support interoperability assessment teams and present written analysis and conclusions in all phases of analysis; develop and analyze system and security documentation; follow up with site administrators for
status on non-compliant platforms and maintain any necessary exception documentation; maintain documentation for exceptions to standards; participate in Security Control Assessments on systems to validate the results of risk assessments and ensure controls in the security plan are present and operating correctly on the system; provides thorough report of the risks to the system and its data; and, evaluate system findings, develop PO&AMs, and briefed stakeholders on key findings, recommendations, risk, and impact.

Minimum Education: Bachelor’s Degree

**Cyber Training Specialist**

Minimum/General Experience: 4

Functional Responsibility: The Cyber Training Specialist develops teaching outlines and determines instructional methods, using knowledge of specific training needs and effectiveness of such methods as individual training, group instruction, lectures, demonstrations, conferences, meetings, or workshops. This individual prepares, organizes and heads training sessions covering standard training, specialized training or counseling in designated areas.

Minimum Education: Bachelor’s Degree

**Incident Response Analyst 3**

Minimum/General Experience: 8

Functional Responsibility: Contributes to generating responses to crisis or urgent situations to mitigate immediate and / or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: lead shifts and functional IR teams, provides oversight for incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets; performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malcode prevention, Firewalls, IDS & IPS, Web security, antispam, etc; performs the role of Incident Coordinator for IT Security events requiring focused response, containment, investigation, and remediation; performs forensic analysis on hosts supporting investigations; conducts malware analysis in out-of-band environment (static and dynamic), including complex malware; coordinate response action to identifies threats and incidents; analyze operational anomalies, network behavior and performs mitigation actions derived from cyber threat monitoring and anomaly analysis, and actively monitors the networks for cybersecurity threats and vulnerabilities; provide oversight and perform quality assurance on Incident Closures; assist with knowledge management - Standard Operating Procedures and procedural support data.

Minimum Education: Bachelor’s Degree

**Penetration Tester I**

Minimum/General Experience: 2

Functional Responsibility: Finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security. Works under immediate supervision and usually reports to a supervisor.

Minimum Education: Bachelor’s Degree

**Cyber Enterprise Architect**

Minimum/General Experience: 4

Functional Responsibility: The Cyber Enterprise Architect works with stakeholders, both leadership and subject matter experts, to build a holistic view of the organization's strategy, processes, information, and information technology assets to ensure that the business and IT are in alignment and protected from cyber threats. The Cyber Enterprise Architect links the business mission, strategy, and processes of an organization to its IT strategy - including
security, and documents this using multiple architectural models or views that show how the current and future needs of an organization will be met in an efficient, sustainable, agile, secure, and adaptable manner.

Minimum Education: Bachelor’s Degree

**Cyber Security Specialist 3**
Minimum/General Experience: 8

Functional Responsibility: The Cyber Security Specialist 3 may identify and resolve highly complex issues to prevent cyber attacks on information systems and to keep computer information systems secure from interruption of service, intellectual property theft, network viruses, data mining, financial theft, and theft of sensitive customer data, allowing business to continue as normal. This is accomplished through the systematic implementation of a cyber framework and process. The Cyber Security Specialist 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. Level 3 is competent in subject matter and concepts and generally considered a specialist in area of assignment. May lead individuals assisting in the work.

Minimum Education: Bachelor’s Degree

**Cyber Security Analyst III**
Minimum/General Experience: 8


Minimum Education: Bachelor’s Degree

**Cyber Security Engineer III**
Minimum/General Experience: 8

Functional Responsibility: Participate in special projects or investigations into specific technology or solution issues and research and piloting of new technologies. Serve as a point of contact for engineering efforts while maintaining compliance with the customer's policies and guidelines. Duties may include: configure and maintain policies; maintain documentation for exceptions to standards; provides timely and adequate response to threats/alerts; assess security events to drive to a resolution; provides timely and sufficient response to security incidents and assessment services; and, promotes security awareness. Cyber Security Engineer III conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, security software engineering, program design, configuration management, integration, and testing of cyber security products and techniques.

Minimum Education: Bachelor’s Degree

**Cyber Malware Reverse Engineer II**
Minimum/General Experience: 4

Functional Responsibility: Assists in investigating potential intrusions and security events to contain and mitigate incidents. Research cyber-attacks, malware, and threat actors to determine potential impact and develop remediation guidance; validate, categorize and investigate escalated cyber security events; profile and trend events in the
environment for potential incidents; collect, assess and catalogue threat indicators; perform malware analysis. Works under general supervision and usually reports to a supervisor, though some ingenuity and flexibility is required.
Minimum Education: Bachelor’s Degree

Cyber Countermeasures Expert II
Minimum/General Experience: 4
Functional Responsibility: Assist with the management and administration of enterprise security programs. Help design and develop countermeasures using advanced knowledge of cyber threats tools, techniques, and processes. Operates with a high level of oversight.
Minimum Education: Bachelor’s Degree

Penetration Tester II -
Minimum/General Experience: 4
Functional Responsibility: Finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security; identification of flaws to cause business risk, a successful candidate provides crucial insights into the most pressing issues and suggests how to prioritize security resources. Works under general supervision and usually reports to a supervisor, though some ingenuity and flexibility is required.
Minimum Education: Bachelor’s Degree

Cybersecurity Subject Matter Expert -I
Responsibility: Under general direction, provides extremely high-level subject matter proficiency for cybersecurity work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems that require doctorate level knowledge of the subject matter for effective implementation.
Educational Requirements: Bachelor’s Degree in Computer Science, Computer Information Systems, Engineering or related field Experience:
Minimum / General - 6 Years’ Experience

Cybersecurity Subject Matter Expert II
Responsibility: Provides extremely high-level subject matter proficiency for cybersecurity work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems that require doctorate level knowledge of the subject matter for effective implementation.
Educational Requirements: Bachelor’s Degree in Computer Science, Computer Information Systems, Engineering or related field Experience:
Minimum / General - 8 Years’ Experience

Cyber Countermeasures Expert II
Minimum/General Experience: 4
Functional Responsibility: Assist with the management and administration of enterprise security programs. Help design and develop countermeasures using advanced knowledge of cyber threats tools, techniques, and processes. Operates with a high level of oversight.
Minimum Education: Bachelor’s Degree
Penetration Tester III -
Minimum/General Experience: 8
Functional Responsibility: Leads the effort in small projects to find security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security; leads the identifying of which key flaws can be exploited to cause business risk, a successful candidate provides crucial insights into the most pressing issues and suggests how to prioritize security resources.
Minimum Education: Bachelor’s Degree

Cyber Malware
Reverse Engineer III Minimum/General Experience: 8
Functional Responsibility: Investigate potential intrusions and security events to contain and mitigate incidents. Research cyber-attacks, malware, and threat actors to determine potential impact and develop remediation guidance; validate, categorize and investigate escalated cyber security events; profile and trend events in the environment for potential incidents; collect, assess and catalogue threat indicators; perform malware analysis. Works under general supervision and usually reports to a supervisor, though some ingenuity and flexibility is required.
Minimum Education: Bachelor’s Degree

Cybersecurity Subject Matter Expert II
Responsibility: Provides extremely high-level subject matter proficiency for cybersecurity work described in the task. Provides advanced technical knowledge and analysis of highly specialized applications and operational environment, high-level functional systems analysis, design, integration, documentation, training, and implementation advice on complex problems that require doctorate level knowledge of the subject matter for effective implementation.
Educational Requirements: Bachelor’s Degree in Computer Science, Computer Information Systems, Engineering or related field Experience:
Minimum / General – 10 Years’ Experience

LABOR CATEGORY RATES GSA SCHEDULE CONTRACT INFORMATION TECHNOLOGY (IT) SERVICES SIN 54151HACS Highly Adaptive Cybersecurity Services (All rates below include IFF)
<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Rate with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Testing and Validation Specialist Cybersecurity</td>
<td>83.23</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst 1</td>
<td>103.35</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Threat Analyst 1</td>
<td>112.75</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incidence Response Analyst</td>
<td>112.75</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Technical Architect 1</td>
<td>117.67</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst I</td>
<td>122.57</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer I</td>
<td>122.57</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst 2</td>
<td>122.57</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist 1</td>
<td>122.57</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Application Architect 1</td>
<td>136.09</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Threat Analyst 2</td>
<td>141.78</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Analyst 2</td>
<td>141.78</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Program Analyst</td>
<td>148.61</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst II</td>
<td>154.56</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst 3</td>
<td>154.56</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist 2</td>
<td>154.56</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer II</td>
<td>154.56</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Application Systems Analyst</td>
<td>157.48</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Operations Manager</td>
<td>160.99</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Technical Architect 2</td>
<td>160.99</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Threat Analyst 3</td>
<td>160.99</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Training Specialist</td>
<td>160.99</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Analyst 3</td>
<td>160.99</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester I</td>
<td>165.14</td>
</tr>
<tr>
<td>SIN</td>
<td>Labor Category</td>
<td>GSA Rate with IFF</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Enterprise Architect</td>
<td>184.07</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist 3</td>
<td>184.07</td>
</tr>
<tr>
<td></td>
<td><strong>Cyber Security Analyst III</strong></td>
<td><strong>184.07</strong></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Engineer III</td>
<td>184.07</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Malware Reverse Engineer II</td>
<td>191.34</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Countermeasures Expert</td>
<td>191.34</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester II</td>
<td>191.34</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Subject Matter Expert 1</td>
<td>207.06</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Subject Matter Expert 2</td>
<td>238.50</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Countermeasures Expert III</td>
<td>243.73</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester III</td>
<td>243.73</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Malware Reverse Engineer III</td>
<td>243.73</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Subject Matter Expert 3</td>
<td>285.75</td>
</tr>
</tbody>
</table>
1. **SCOPE**

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

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.

**Measured Service requirement in Table 2, below.**

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 MAS 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

2. DESCRIPTION OF CLOUD COMPUTING SERVICES (i.e. IaaS, etc.) AND PRICING

a. Service Description Requirements for Listing Contractors

The description requirements below are in addition to the overall Schedule 70 evaluation criteria described in SCP-FSS-001-N Instructions Applicable to New Offerors (Alternate I-MAR 2016) or SCP-FSS-001-S Instructions Applicable to Successful FSS Program Contractors, as applicable, SCP-FSS-004 and other relevant publications.

Refer to overall Schedule 70 requirements for timelines related to description and other schedule updates, including but not limited to clauses 552.238-81 section E and clause I-FSS-600.

Table 2 summarizes the additional Contractor-provided description requirements for services proposed under the Cloud Computing Services (i.e IaaS, etc.). All mandatory description requirements must be complete, and adequate according to evaluation criteria.

In addition there is one Optional reporting descriptions which exists to provide convenient service selection by relevant criteria. Where provided, optional description requirements must be complete and adequate according to evaluation criteria:

(1) The NIST Service Model provides sub-categories for the Cloud SIN and is strongly encouraged, but not required. The Service Model based sub-categories provide this SIN with a structure to assist ordering activities in locating and comparing services of interest. Contractors may optionally select the single service model most closely corresponding to the specific service offering.

(2) If a sub-category is selected it will be evaluated with respect to the NIST Service
Model definitions and guidelines in Guidance for Contractors

Table 2: Cloud Service Description Requirements

<table>
<thead>
<tr>
<th>#</th>
<th>Description Requirement</th>
<th>Reporting Type</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Provide a brief written description of how the proposed cloud computing services (i.e. IaaS, etc.) satisfies each individual essential NIST Characteristic</td>
<td>Mandatory</td>
<td>The cloud service must be capable of satisfying each of the five NIST essential Characteristics as outlined in NIST Special Publication 800-145. See ‘GUIDANCE FOR CONTRACTORS: NIST Essential Characteristics’ below in this document for detailed overall direction, as well as guidance on inheriting essential characteristics. The NIST “Measured Service” characteristic requires a minimal “pay as you go” unit of measurement appropriate for the service. In the case of SaaS, the appropriate maximum measured increment of service shall be no more than 30 days per user, or some other equivalent discrete measurement that provides the government with the advantage of frequent (approximately every 30 days) “pay as you go” metering cycles. SaaS products, where consumption is only measured on an annual basis, may better fit under “Term Software License” SIN 132-32. Likewise, offers of any combinations of IaaS, PaaS or any other cloud product</td>
</tr>
</tbody>
</table>
2. **RESPONSIBILITIES OF THE CONTRACTOR**

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

a. **Acceptance Testing**

Any required Acceptance Test Plans and Procedures shall be negotiated by the Ordering Activity at task order level. The Contractor shall perform acceptance testing of the systems for Ordering Activity approval in accordance with the approved test procedures.

b. **Training**

If training is provided commercially the Contractor shall provide normal commercial installation, operation, maintenance, and engineering interface training on the system. Contractor is responsible for indicating if there are separate training charges.

c. **Information Assurance/Security Requirements**

The contractor shall meet information assurance/security requirements in accordance with the Ordering Activity requirements at the Task Order level.

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select NIST deployment models for the cloud computing service proposed.</td>
<td>Optionally select the most appropriate NIST service model that will be the designated sub-category, or may select no sub-category.</td>
</tr>
<tr>
<td></td>
<td>Mandatory</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>Contractors must select at least one NIST deployment model as outlined in NIST Special Publication 800-145 describing how the proposed cloud computing service is deployed. Select multiple deployment models if the service is offered in more than one deployment model. See ‘GUIDANCE FOR CONTRACTORS: NIST Deployment Model’ below in this document for detailed direction on how to best categorize a service for the NIST deployment models.</td>
<td>Contractor may select a single NIST Service model to sub-categorize the service as outlined in NIST Special Publication 800-145. Sub-category selection is optional but recommended. See ‘GUIDANCE FOR CONTRACTORS: NIST Service Model’ below in this document for detailed direction on how to best categorize a service for the NIST IaaS, PaaS, and SaaS service models.</td>
</tr>
</tbody>
</table>
d. **Related Professional Services**
The Contractor is responsible for working with the Ordering Activity to identify related professional services and any other services available on other SINs that may be associated with deploying a complete cloud solution. Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN.

e. **Performance of Cloud Computing Services**
The Contractor shall respond to Ordering Activity requirements at the Task Order level with proposed capabilities to Ordering Activity performance specifications or indicate that only standard specifications are offered. In all cases the Contractor shall clearly indicate standard service levels, performance and scale capabilities.

The Contractor shall provide appropriate cloud computing services on the date and to the extent and scope agreed to by the Contractor and the Ordering Activity.

f. **Reporting**
The Contractor shall respond to Ordering Activity requirements and specify general reporting capabilities available for the Ordering Activity to verify performance, cost and availability.

In accordance with commercial practices, the Contractor may furnish the Ordering Activity/user with a monthly summary Ordering Activity report.

3. **RESPONSIBILITIES OF THE ORDERING ACTIVITY**

The Ordering Activity is responsible for indicating the cloud computing services requirements unique to the Ordering Activity. Additional requirements should not contradict existing SIN or MAS Terms and Conditions. Ordering Activities should include (as applicable) Terms & Conditions to address Pricing, Security, Data Ownership, Geographic Restrictions, Privacy, SLAs, etc.

Cloud services typically operate under a shared responsibility model, with some responsibilities assigned to the Cloud Service Provider (CSP), some assigned to the Ordering Activity, and others shared between the two. The distribution of responsibilities will vary between providers and across service models. Ordering activities should engage with CSPs to fully understand and evaluate the shared responsibility model proposed. Federal Risk and Authorization Management Program (FedRAMP) documentation will be helpful regarding the security aspects of shared responsibilities, but operational aspects may require additional discussion with the provider.

a. **Ordering Activity Information Assurance/Security Requirements Guidance**

(1) The Ordering Activity is responsible for ensuring to the maximum extent practicable that each requirement issued is in compliance with the Federal Information Security Management Act (FISMA) as applicable.
The Ordering Activity shall assign a required impact level for confidentiality, integrity and availability (CIA) prior to issuing the initial statement of work. The Contractor must be capable of meeting at least the minimum security requirements assigned against a low-impact information system in each CIA assessment area (per FIPS 200) and must detail the FISMA capabilities of the system in each of CIA assessment area.

Agency level FISMA certification, accreditation, and evaluation activities are the responsibility of the Ordering Activity. The Ordering Activity reserves the right to independently evaluate, audit, and verify the FISMA compliance for any proposed or Awarded Cloud Computing Services.

The Ordering Activity has final responsibility for assessing the FedRAMP status of the service, complying with and making a risk-based decision to grant an Authorization to Operate (ATO) for the cloud computing service, and continuous monitoring. A memorandum issued by the Office of Management and Budget (OMB) on Dec 8, 2011 outlines the responsibilities of Executive departments and agencies in the context of FedRAMP compliance.

Ordering activities are responsible for determining any additional information assurance and security related requirements based on the nature of the application and relevant mandates.

b. Deployment Model

If a particular deployment model (Private, Public, Community, or Hybrid) is desired, Ordering Activities are responsible for identifying the desired model(s). Alternately, Ordering Activities could identify requirements and assess Contractor responses to determine the most appropriate deployment model(s).

c. Delivery Schedule

The Ordering Activity shall specify the delivery schedule as part of the initial requirement. The Delivery Schedule options are found in Information for Ordering Activities Applicable to All Special Item Numbers.

d. Interoperability

Ordering Activities are responsible for identifying interoperability requirements. Ordering Activities should clearly delineate requirements for API implementation and standards conformance.

e. Performance of Cloud Computing Services

The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.
f. Reporting

The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of
the initial requirement.

g. Privacy

The Ordering Activity should specify the privacy characteristics of their service and engage with the
Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For
example, a requirement could be requiring assurance that the service is capable of safeguarding
Personally Identifiable Information (PII), in accordance with NIST SP 800-122\(^4\) and OMB memos M-
06-16\(^5\) and M-07-16\(^6\). An Ordering Activity will determine what data elements constitute PII
according to OMB Policy, NIST Guidance and Ordering Activity policy.

h. Accessibility

The Ordering Activity should specify the accessibility characteristics of their service and engage with the
Contractor to determine the cloud service is capable of meeting Ordering Activity requirements. For
example, a requirement could require assurance that the service is capable of providing accessibility based

i. Geographic Requirements

Ordering activities are responsible for specifying any geographic requirements and engaging with the
Contractor to determine that the cloud services offered have the capabilities to meet geographic
requirements for all anticipated task orders. Common geographic concerns could include whether service
data, processes and related artifacts can be confined on request to the United States and its territories, or
the continental United States (CONUS).

j. Data Ownership and Retrieval and Intellectual Property

Intellectual property rights are not typically transferred in a cloud model. In general, CSPs retain
ownership of the Intellectual Property (IP) underlying their services and the customer retains ownership
of its intellectual property. The CSP gives the customer a license to use the cloud services for the duration
of the contract without transferring rights. The government retains ownership of the IP and data they
bring to the customized use of the service as spelled out in the FAR and related materials.

General considerations of data ownership and retrieval are covered under the terms of Schedule 70 and
the FAR and other laws, ordinances, and regulations (Federal, State, City, or otherwise). Because of
considerations arising from cloud shared responsibility models, ordering activities should engage with
the Contractor to develop more cloud-specific understandings of the boundaries between data owned by
the government and that owned by the cloud service provider, and the specific terms of data retrieval.
In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government.

The Ordering Activity should expect that the Contractor shall transfer data to the government at the government's request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service. Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government's use of the cloud provider's service.
- Virtual machine configurations created by the government but operating on the cloud provider's service.
- Profile, configuration and other metadata used to configure SaaS application services or PaaS platforms.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

k. Service Location Distribution

The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

1. Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.
2. Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors.

Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

l. Related Professional Services

Ordering activities should engage with Contractors to discuss the availability of limited assistance with initial setup, training and access to the services that may be available through this SIN.
Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN. Ordering activities should consult the appropriate GSA professional services schedule.

m. Performance of Cloud Computing Services

The Ordering Activity should clearly indicate any custom minimum service levels, performance and scale requirements as part of the initial requirement.

n. Reporting

The Ordering Activity should clearly indicate any cost, performance or availability reporting as part of the initial requirement.

o. Privacy

The Ordering Activity should specify the privacy characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could be requiring assurance that the service is capable of safeguarding Personally Identifiable Information (PII), in accordance with NIST SP 800-122\textsuperscript{4} and OMB memos M-06-16\textsuperscript{5} and M-07-16\textsuperscript{6}. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy.

p. Accessibility

The Ordering Activity should specify the accessibility characteristics of their service and engage with the Contractor to determine if the cloud service is capable of meeting Ordering Activity requirements. For example, a requirement could require assurance that the service is capable of providing accessibility based on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d).

q. Geographic Requirements

Ordering activities are responsible for specifying any geographic requirements and engaging with the Contractor to determine that the cloud services offered have the capabilities to meet geographic requirements for all anticipated task orders. Common geographic concerns could include whether service data, processes and related artifacts can be confined on request to the United States and its territories, or the continental United States (CONUS).

r. Data Ownership and Retrieval and Intellectual Property
In all cases, the Ordering Activity should enter into an agreement with a clear and enforceable understanding of the boundaries between government and cloud service provider data, and the form, format and mode of delivery for each kind of data belonging to the government.

The Ordering Activity should expect that the Contractor shall transfer data to the government at the government's request at any time, and in all cases when the service or order is terminated for any reason, by means, in formats and within a scope clearly understood at the initiation of the service. Example cases that might require clarification include status and mode of delivery for:

- Configuration information created by the government and affecting the government’s use of the cloud provider’s service.
- Virtual machine configurations created by the government but operating on the cloud provider’s service.
- Profile, configuration and other metadata used to configure SaaS application services or PaaS platform services.

The key is to determine in advance the ownership of classes of data and the means by which Government owned data can be returned to the Government.

5. Service Location Distribution

The Ordering Activity should determine requirements for continuity of operations and performance and engage with the Contractor to ensure that cloud services have adequate service location distribution to meet anticipated requirements. Typical concerns include ensuring that:

1. Physical locations underlying the cloud are numerous enough to provide continuity of operations and geographically separate enough to avoid an anticipated single point of failure within the scope of anticipated emergency events.
Service endpoints for the cloud are able to meet anticipated performance requirements in terms of geographic proximity to service requestors.

Note that cloud providers may address concerns in the form of minimum distance between service locations, general regions where service locations are available, etc.

t. Related Professional Services

Ordering activities should engage with Contractors to discuss the availability of limited assistance with initial setup, training and access to the services that may be available through this SIN.

Any additional substantial and ongoing professional services related to the offering such as integration, migration, and other cloud professional services are out of scope for this SIN. Ordering activities should consult the appropriate GSA professional services schedule.

**Cloud - Applications Development Analyst**
Responsibilities (within the context of Cloud development/deployment): Understands the business needs of the client and translates that knowledge into highly useful applications for the client (Web, desktop, or mobile). Works (either alone or as a team member) using sound and proven technologies to deliver a quality product. Actively participates in the needs assessment process. Responsible for designing, coding, testing, implementing, maintaining and supporting applications software. Responsible for providing possible technical solutions to development obstacles.

Minimum/General Experience: Typically has 2 years of experience

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems or other related field; or equivalent work experience

**Cloud - Applications Architect-Entry**
Has extensive knowledge of the long-term business and technical needs of the client and provides enterprise level solutions accordingly.

Minimum/General Experience: 3 years Experience

Minimum Education: Bachelor’s Degree in Computer Science, Information Systems or other related field; or equivalent work experience.

---

**LABOR CATEGORY RATES GSA SCHEDULE CONTRACT INFORMATION TECHNOLOGY (IT) SERVICES SIN**
<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Rate with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>518210C</td>
<td>Cloud Applications Development Analyst-Entry</td>
<td>61.93</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Quality Assurance Analyst -Intermediate</td>
<td>71.45</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Applications Architect- Entry</td>
<td>80.98</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Applications Development Analyst Intermediate</td>
<td>85.75</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Quality Assurance Analyst -Advanced</td>
<td>90.51</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Database Administrator-Intermediate</td>
<td>110.49</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Applications Architect- Intermediate</td>
<td>95.54</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Applications Development Analyst Advanced</td>
<td>110.21</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Applications Architect- Intermediate</td>
<td>111.47</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Application Architect-Advanced</td>
<td>110.16</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Database Administrator-Advance</td>
<td>95.54</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Architect- Advanced</td>
<td>93.59</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Project Manager- Intermediate</td>
<td>119.11</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Project Manager- Advanced</td>
<td>123.86</td>
</tr>
</tbody>
</table>
1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 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.

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)
   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

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

4. PERFORMANCE OF SERVICES
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
   b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
   c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

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

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

(1) Cancel the stop-work order; or

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

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

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

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

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

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

6. INSPECTION OF SERVICES

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

7. RESPONSIBILITIES OF THE CONTRACTOR

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

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

9. INDEPENDENT CONTRACTOR

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

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

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

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

11. INVOICES

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

12. PAYMENTS

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

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

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

1. The offeror;
2. Subcontractors; and/or
3. Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

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

15. APPROVAL OF SUBCONTRACTS

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 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 DESCRIPTIONS
SIN 54151S
INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

Project Manager:
Responsibilities: Project budgeting and financial oversight. Reports directly to client stakeholders on matters related to the project including resource allocation, project development milestones, change management, and budget. Provides direct management to all team members, including the development team, to ensure that the project reaches a
satisfactory conclusion. Schedules and prioritizes all task development. Works with the client to clear development bottlenecks and provide solutions to complex problems in order to keep the project progressing to a successful conclusion.

Minimum/General Experience: Typically has 3 years of experience as a Senior Business Analyst (with some project management experience within this role)
Minimum Education: Bachelor's Degree in Computer Science, Information Systems, Business Administration, or related field; or equivalent work experience.

Program Manager
Responsibilities: Performs day-to-day management of delivery order projects for ERP technology projects that involve teams of data processing and other information systems management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, convening, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. organizes, directs, and coordinates the planning and production of all activities associated with assigned deliverables. Establishes and alters, as necessary, corporate management structure to direct effective contract support activities. Demonstrates good written and oral communications.
Experience: Must have 10 years of IT experience, including at least 7 years of IT and/or telecommunications system management experience.
Education: B.A. or B.S. degree. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

Database Administrator 1:
Responsibilities: Assists advanced DBAs in the Installation and maintenance of database instances. Performs database design, implementing and management, data migration and specialized data handling. Performs database backup and recovery. Assists advanced DBAs to ensure that the proper security and authentication protocols/expectations of the client are met. Conducts performance monitoring and tuning (including query formation). Trouble-shoots performance bottlenecks (including query formation).
Minimum/General Experience: Typically has 4 years of experience as a Database Administrator
Minimum Education: Bachelor’s Degree in Computer Science, Information Systems or other related field; or equivalent work experience.

Database Administrator 2:
Responsibilities: Oversees the Installation and maintenance of database instances. Performs data migration and specialized data handling. Engineers, directs and performs database backup and recovery. Ensures that the proper security and authentication protocols/expectations of the client are met. Ensures that the database infrastructure is implemented in a scalable fashion to react to specific and changing capacity requirements. Conducts performance monitoring and tuning (including query formation). Trouble-shoots performance bottlenecks (including query formation). Provides direction to Cloud Engineers and may provide management of their daily activities.
Experience: Typically has 6+ years of experience as an Database Administrator.
Education: Bachelor's Degree in Computer Science, Information Systems or other
related field; or equivalent work experience.

**Network Engineer:**

**Responsibilities:** plans, supports and evaluates complex existing network systems and make recommendations for resources required to maintain and/or expand service levels. This resource will provide highly skilled technical assistance in network planning, engineering and architecture. Plans and incorporates how new network resources and applications will exist on the network. Provide monthly metrics for network availability and bandwidth usage as well as other metrics as requested. Responsible for network capacity planning, user support, and escalation of issues to upper tiers. Use network management tools to discover, map and maintain the network. Responsible for network equipment OS and version upgrades. Maintain Internet and Extranet connectivity; handles day-to-day Firewall administration, as well as VPN connectivity. Monitor and maintain network interfaces to insure its highest level of performance and makes modifications and enhancements as needed. Responsible for documenting procedures and keeping network diagrams and related material up to date. Handle user problems, questions, and request on network issues. Work with other groups within IS to resolve network related issues as needed.

**Experience:** Requires at least 2 years relevant experience.

**Education:** B.S. or B.A. degree in Computer Science, Engineering or related fields (or equivalent experience).

**Software Engineer Junior:**

**Responsibilities:** be responsible for learning existing/legacy system architecture, design, functions and capabilities to support the design and implementation of new capabilities and enhancements

**Experience:** 2 Years

**Education:** BS degree or equivalent experience and less than 2 years prior relevant experience.

**Software Engineer Senior:**

**Experience:** 2 Years

**Education:** BS degree or equivalent experience and less than 2 years prior relevant experience

**Systems Analyst:**

Responsibilities: Under close supervision gathers facts, analyses data, compares alternatives in terms of cost, time and availability of equipment/personnel. Supports determination and resolution of data processing problems and coordinates work

**Experience:** This is the entry level position for this job category.

**Education:** B.A. or B.S. degree in Computer Science, Engineering, Business or a related field. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.

**Systems Engineer Junior:**

Responsibilities: Provides technical support in system architecture, system design, system integration and technical management. Assists in providing technical input to the systems engineering process. May assist in developing and implementing installation plans. May assist in preparation and presentation of systems assurance reviews. Identifies requirements and deficiencies in hardware and software products,

**Experience:** At least 2 years of relevant experience.

**Education:** B.A. or B.S. degree in Computer Science, Engineering or a related field or equivalent experience. Five (5) years of direct related experience in a related field may be substituted for a Bachelor's degree requirement.
**Systems Engineer Senior:**

Responsibilities: Capture, Requirements Management, System Design Documents, Trade Studies, and Research and Authoring of White Papers. Devise new approaches to resolve complex engineering problems and conduct feasibility studies. Formulate plans based on the development of innovative new designs/solutions to meet customer needs. Provide technical leadership for the integration of requirements, design, and technology. Develop system architecture and system design documentation.

Required education: Bachelor Degree in computer science/information technology or related field

Experience: 10+ years of relevant experience or (8+ years with a Master’s Degree)

**Applications Developer 1**

Responsibilities: strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant may apply their core skills and/or specific IT skills on projects. They may direct small teams and interact with the clients at the supervisory level.

Education: Bachelor’s Degree or 3 years additional related experience

Experience: 2 to 6 years of experience

**Applications Developer 2**

Responsibilities: Apply their strong analytical and technical skills to assist in implementing IT business solutions. An IT Consultant may apply their core skills and/or specific IT skills on projects. They direct teams and interact with the clients at the supervisory or program level.

Education: Bachelor’s Degree or 3 years additional related experience

Experience: 2 to 6 years of experience

**Junior Test Engineer:**

Responsibilities: includes performing systems requirements, functional and timeline analysis, trade studies, requirements allocation, interface definition, technical oversight, integration, system testing, and quality assurance and additional duties, as needed, to support the team.

Experience: 3 Years

Education: BA/BS in software engineering/development, computer science, information technology, and 3+ years of relevant experience or Masters with at least one year of prior relevant experience.
<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Rate with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>IT Project Manager</td>
<td>127.71</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Program Manager</td>
<td>155.74</td>
</tr>
<tr>
<td>54151S</td>
<td>Database Management Specialist 1</td>
<td>96.25</td>
</tr>
<tr>
<td>54151S</td>
<td>Database Management Specialist 2</td>
<td>152.09</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer</td>
<td>110.70</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer Junior</td>
<td>77.01</td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer Senior</td>
<td>147.27</td>
</tr>
<tr>
<td>54151S</td>
<td>System Analyst</td>
<td>97.44</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer</td>
<td>82.90</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer Senior</td>
<td>160.85</td>
</tr>
<tr>
<td>54151S</td>
<td>Application Developer 1</td>
<td>103.52</td>
</tr>
<tr>
<td>54151S</td>
<td>Application Developer 2</td>
<td>122.42</td>
</tr>
<tr>
<td>54151S</td>
<td>Junior Test Engineer</td>
<td>73.11</td>
</tr>
</tbody>
</table>
Vendor suitability for offering services through the new Health IT SIN must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications
- Federal Information Security Management Act (FISMA) of 2002

1. SCOPE
   a. The labor categories, prices, terms and conditions stated under Special Item Number 54151HEAL Health Information Technology Services apply exclusively to Health IT Services within the scope of this Information Technology Schedule.
   b. This SIN is limited to Health IT Services only. Software and hardware products are out of scope. Hardware and software can be acquired through different Special Item Numbers on MAS.
   c. This SIN provides ordering activities with access to Health IT services.
   d. Health IT Services provided under this SIN shall comply with all Healthcare certifications and industry standards as applicable at the task order level.
   e. The Contractor shall provide services at the Contractor’s facility and/or at the

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.

4. PERFORMANCE OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS
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 (Deviation – May 2003) Rights in Data – General, may apply.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite Health IT Services.

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

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

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

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.
To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

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

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

11. 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.

12. 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.

13. DESCRIPTION OF IT SERVICES AND PRICING
a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151S IT 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 Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.
<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Rate with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HEAL</td>
<td>Health IT Applications Development Analyst - Entry</td>
<td>61.93</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Quality Assurance Analyst - Intermediate</td>
<td>71.45</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Applications Architect – Entry</td>
<td>80.98</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Applications Architect – Entry</td>
<td>85.75</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Business Analyst-Intermediate</td>
<td>85.75</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Quality Assurance Analyst-Advanced</td>
<td>90.51</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Database Administrator-Intermediate</td>
<td>94.32</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Applications Architect-Intermediate</td>
<td>95.27</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Applications Development Analyst-Advanced</td>
<td>100.04</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Business Analyst-Advanced</td>
<td>100.04</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Database Administrator-Advanced</td>
<td>109.57</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Applications Architect-Advanced</td>
<td>109.57</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Project Manager-Intermediate</td>
<td>119.10</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Healthcare IT Project Manager-Advanced</td>
<td>123.85</td>
</tr>
</tbody>
</table>
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION
PROCUREMENT PROGRAMS

PREAMBLE
ICS provides commercial products and services to ordering activities. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT
To actively seek and partner with small businesses.
To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.
To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.
To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.
To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.
To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.
To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.
We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact us at:

z SofTech Solutions, INC
235 Peachtree Street, Suite 400
Atlanta, GA 30303
www.zsoftechsolutions.com
678-778-7817
BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) ________________.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations, and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the ordering activity that works better and costs less.

Signatures

Ordering Activity ____________________________ Date ________________

Contractor ____________________________ Date ________________
BLANKET PURCHASE AGREEMENT

Pursuant to GSA Federal Supply Schedule Contract Number(s) ______________, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (ordering activity):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

<table>
<thead>
<tr>
<th>MODEL NUMBER/PART NUMBER</th>
<th>*SPECIAL BPA DISCOUNT/PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(2) Delivery:

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>DELIVERY SCHEDULES / DATES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(3) The ordering activity estimates, but does not guarantee, that the volume of purchases through this agreement will be ____________________________.

(4) This BPA does not obligate any funds.

(5) This BPA expires on _________________ or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA:

<table>
<thead>
<tr>
<th>OFFICE</th>
<th>POINT OF CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;
(b) Contract Number;
(c) BPA Number;
(d) Model Number or National Stock Number (NSN);
(e) Purchase Order Number;
(f) Date of Purchase;
(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and

(h) Date of Shipment.

(9) The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor’s invoice, the provisions of this BPA will take precedence.

*******************************************************************************************
BASIC GUIDELINES FOR USING
“CONTRACTOR TEAM ARRANGEMENTS”

Federal Supply Schedule Contractors may use “Contractor Team Arrangements” (see FAR 9.6) to provide solutions when responding to a ordering activity requirements.

These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts.

Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors.

Customers should refer to FAR 9.6 for specific details on Team Arrangements.

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customers needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.