Note: Contractor has been awarded all Special Item Numbers under the Cooperative Purchasing and Disaster Recovery Programs.

SIN 54151S - Information Technology Professional Services
SIN 54151HACS – HIGHLY ADAPTIVE CYBERSECURITY SERVICES
SIN - ORDER LEVEL MATERIALS (OLM)

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.

Tetrad Digital Integrity LLC
1155 Connecticut Avenue NW, 11th Floor
Washington, DC 20036
Phone: (202) 337-5600  Fax: (202) 337-5601
Internet Address: http://www.tdisecurity.com/

Contract Number:
GS-35F-0414U

Period Covered by Contract:

May 28, 2018 Through May 27, 2023

General Services Administration
Federal Acquisition Service
Pricelist current through Schedule 70 MAS consolidation 47QSMD20R0001, dated 6 February 2020

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Acquisition Service’s Home Page via the Internet at http://www.gsa.gov/fas
TABLE OF CONTENTS

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS .........................3

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBER 132-45) ........................................................................................................7

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51) ........................................................................................................11

TETRAD DIGITAL INTEGRITY LLC’S LABOR CATEGORY DESCRIPTIONS AND RATES FOR ALL AWARDED SINS ..................................................................................................................15
<table>
<thead>
<tr>
<th>INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a. Table of awarded special item number with appropriate cross-reference to item descriptions and awarded prices. <em>See pricing for Special Item Numbers 54151HACS, 54151S, &amp; OLM</em></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>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. <em>See pricing for Special Item Numbers 54151HACS, 54151S, &amp; OLM</em></td>
</tr>
<tr>
<td>2. Maximum order: SINs 54151HACS &amp; 54151S132-45 &amp; 132-51: $500,000; SIN OLM: $250,000</td>
</tr>
<tr>
<td>3. Minimum order: All Awarded SINS: $100</td>
</tr>
<tr>
<td>4. Geographic coverage (delivery area): <em>Domestic Delivery Only</em></td>
</tr>
<tr>
<td>5. Point(s) of production (city, county, and State or foreign country): <em>Washington, DC</em></td>
</tr>
<tr>
<td>6. Discount from list prices or statement of net price: <em>Prices listed are net</em></td>
</tr>
<tr>
<td>7. Quantity discounts: <em>None</em></td>
</tr>
<tr>
<td>8. Prompt payment terms: <em>None – Net 30 days from receipt of invoice or date of acceptance, whichever is later.</em></td>
</tr>
<tr>
<td>9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold.</td>
</tr>
<tr>
<td>9b. Notification that Government purchase cards are accepted or not accepted above the micro-purchase threshold.</td>
</tr>
<tr>
<td>10. Foreign items (list items by country of origin): <em>Not Applicable</em></td>
</tr>
<tr>
<td>11a. Time of delivery: <em>As Negotiated for all awarded SINS</em></td>
</tr>
<tr>
<td>11b. Expedited Delivery: <em>Contact Contractor</em></td>
</tr>
</tbody>
</table>
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. point: Destination

13a. Ordering address:

**Tetrad Digital Integrity LLC**
1155 Connecticut Avenue NW, 11th Floor
Washington, DC 20036

13b. Ordering procedures: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

14. Payment address:

**Tetrad Digital Integrity LLC**
1155 Connecticut Avenue NW, 11th Floor
Washington, DC 20036

15. Warranty provision: Not Applicable

16. Export packing charges, if applicable: Not Applicable

17. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level): Not Applicable

18. Terms and conditions of rental, maintenance, and repair (if applicable): Not Applicable

19. Terms and conditions of installation (if applicable): Not Applicable

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

20a. Terms and conditions for any other services (if applicable): Not Applicable

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

22. List of participating dealers (if applicable): Not Applicable

23. Preventive maintenance (if applicable): Not Applicable
24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): *Not Applicable*

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. contractor’s website or other location.) The EIT standards can be found at: www.Section508.gov/.

25. Data Universal Number System (DUNS) number: 031585099

26. Notification regarding registration in the System for Award Management. *CAGE Code 1UR58*
Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M- 19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

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 IT Schedule 70 (e.g. 511210, 33411), 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 subcategory include Network Mapping,
Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

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

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY
   Subject to the ordering activity 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
a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Number 54151HACS for Highly Adaptive Cybersecurity Services and it should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

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

EXAMPLE

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

Professionals involved in this specialty perform the following tasks:

▪ Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
▪ Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
▪ Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

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

Minimum Experience: 5 Years

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

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 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**

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
See Labor Category descriptions included herein.
Disaster Recovery Specialist  

GSA Rate: $91.20

**Functional Responsibility:** Responsible for managing the implementation of disaster recovery plans. Develops plans to continue information systems functions. Has knowledge and experience related to requirements for data, computers, communications, personnel requirements, processing schedules, and regulatory and legal responsibilities. Works with client to arrange off-site facilities for data archiving, storage, and access. Possesses experience related to the requirements of appropriate off-site facilities and equipment for resuming computer operations in the event of a disaster. Has knowledge of industry security practices and the ability to establish notification processes for communicating in the event of emergencies. Implements and coordinates tests of disaster recovery plans and procedures. Coordinates the development and implementation of disaster recovery operations with local and government emergency agencies and external service providers.

**Minimum/General Experience:**
- 3 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Security Analyst  

GSA Rate: $92.54

**Functional Responsibility:** Responsible for researching, examining, reporting, and analyzing security incidents and related reports. Capable of analysis of malicious codes, vulnerable software, security tools, and patches. Develops technical content for technical documents, including content such as incident/vulnerability notes, advisories, and technical guidelines. Works on the development of white papers describing best practices for system and network administrators, technology managers, and other technology professionals. May support development of Certification and Accreditation documentation.

**Minimum/General Experience:**
- 3 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Senior Systems Consultant  

GSA Rate: $97.73

**Functional Responsibility:** Responsible for systems engineering, process engineering, network engineering or systems applications. Understands aspects of network and systems standards and architectures or process re-engineering techniques and methodologies. Skilled information technology professional. Might serve as systems architect. Provides high level understanding and guidance of systems implementation or process re-engineering.

**Minimum/General Experience:**
- 4 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Data Security Specialist

Functional Responsibility: Directs and implements controls and procedures to cost-effectively protect information systems assets from intentional or inadvertent modification, disclosure or destruction. Provides guidance and direction for the protection of information systems assets. Provides reports to managers regarding effectiveness of data security. Makes recommendations for the adoption of new procedures and may assign work to staff and monitor performance.

Minimum/General Experience:
- 3 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field

GSA Rate: $109.28

Security Engineer

Functional Responsibility: Typically works under technical supervision and mentorship of senior security engineers. Must have experience in 3 or more of the following skill areas: Certification and Accreditation, DITSCAP, DIACAP, NIACAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Systems Engineering, UNIX and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/P, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing

Minimum/General Experience:
- 2 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field

GSA Rate: $112.39

Forensics / Security Incident Expert

Functional Responsibility: Performs tasks which include: document and file discovery that involves the ability to locate and recover previously inaccessible documents and files through computer forensic processes. Capable of data recovery and analysis that includes the ability to access data storage devices using recovery and analysis tools and techniques to recover active and deleted data from inaccessible media and deleted files, including email. Provides restoration of data that requires recovery from a variety of storage media and operating systems analyses data. Uses tools and techniques to access password protected files and hard drives. Provides detailed reports about data collected and produced to support the case. Knowledgeable about standard forensic data collection methodologies.

Minimum/General Experience:
- 5 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field

GSA Rate: $123.15
Certification & Accreditation (C&A) Specialist

**Functional Responsibility:** Performs Information Assurance (IA) consulting, assessment, documentation and IA compliance program development. Deals with programs which must comply with or follow guidance of Federal Information Security Management Act (FISMA), OMB A-130, NIST SP 800 Series, NIST FIPS Publications, DCID 6/3, NISCAP, and/or DoD DITSCAP or DIACAP programs. Assist in Certification and Accreditation (C&A) process negotiation and task management for accomplishing C&A activities. Prepares and updates C&A packages to obtain or maintain Authority-to-Operate (ATO) approval. Prepares the System Security Plan (SSP), System Security Authorization Agreement (SSAA), or the Application Security Plan (ASP), as appropriate, for C&A package submission. Prepares quarterly FISMA compliance reports as required. Prepares Privacy Impact Assessments (PIA) as necessary. Prepares and conducts Security Test and Evaluation (ST&E) for supported systems. Analyzes results of ST&E to produce Plan of Action and Milestones (POA&M).

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Information Assurance (IA) Policy Specialist

**Functional Responsibility:** Provides regulatory guidance for Information Assurance (IA), including advice on how to adhere to national, executive, civil, DoD and organizational security requirements such as The Federal Information Security Management Act of 2002 (FISMA). Responsible for interpreting IA requirements using DoD, FISMA, and NIST guidelines. Familiar with and experienced in completing NIST and/or DITSCAP/DIACAP C&A processes. Responsible for policy compliance, internal policy development, and strategic planning. Typically, responsible for monitoring compliance notices and ensuring that security patches, communication tasking orders and warning orders are known. Provides guidance and requirements insight on IA topics such as PKI integration, Common Access Card (CAC) authentication, vulnerability scanning, and DoD 8500 security controls compliance.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Senior Security Engineer

**Functional Responsibility:** Ability to work independently with minimal technical oversight. Must have experience in 5 or more of the following skill areas: Certification and Accreditation, DITSCAP, DIACAP, NIASP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Systems Engineering, UNIX and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Lead Security Engineer

GSA Rate: $171.03

**Functional Responsibility:** Certified Information Security Specialist Professional (CISSP). Ability to work independently as a Project Manager or Technical Task Leader. Recognized as an Information Assurance (IA) Subject Matter Expert (SME) through in-depth experience, technical speaking engagements and/or published articles. In-depth knowledge of government IA requirements, documentation & procedures. Demonstrated ability to plan IA tasks and assign resources to meet customer requirements. Must have experience in 7 or more of the following skill areas: Certification and Accreditation, DITSCAP, DIACAP, NIACAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Systems Engineering, UNIX and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/P, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

**Minimum/General Experience:**
- 8 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Security Assessment Expert

GSA Rate: $183.25

**Functional Responsibility:** Focused on security assessments, vulnerability assessments, risk assessments, penetration testing, and/or network and host scanning. Understands methodologies and tools for assessing the security of systems, applications, and/or networks. Relies on one or more methodologies/frameworks for assessing security, such as those published by OWASP or NIST. Able to interpret results of assessments and develop plans for remediation of discovered vulnerabilities.

**Minimum/General Experience:**
- 8 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Subject Matter Expert

GSA Rate: $244.33

**Functional Responsibility:** Provides expert consultation and direction for information assurance/security. Subject Matter Expert (SME) is typically used for expert opinion and counsel and often has a specific field of expertise. Recognized as a SME through in-depth experience, technical speaking and/or training engagements, and/or published articles. Often lectures on various topics at conferences, formal classrooms, and in corporate settings.

**Minimum/General Experience:**
- 10 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Technology Lead

**GSA Rate:** $128.04

**Functional Responsibility:** Take a lead role in conducting research and analysis on IT industry emerging trends and developments and make recommendations on technologies and techniques to be employed to support customer requirements and mission goals. Lead in the review of relevant technologies and be able to assess and prepare technical specifications, work requirements, and/or other acquisition related documentation. Develop draft project plans, operating plans and/or supporting budgets; and determine scope, methods, and resource requirements and schedules for IT projects and supporting analyses.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

---

IT Administrator

**GSA Rate:** $84.15

**Functional Responsibility:** Review, aggregate, and interpret various network and operating system logs, as well as prepare reports to highlight issues, suspicious activities, risks, and other pertinent information regarding the operation and configuration of systems and networks. Familiar with reading access control lists on Cisco products, as well as various Microsoft, Solaris, UNIX and/or Novell operating system logs. Experience in the use of various professional tools that can extract and/or interpret data, such as but not limited to, UNIX commands such as grep and awk. Familiarity with system management tools including Ciscoworks and possess an ability to accurately and effectively perform system and network administrative work that is detail oriented.

**Minimum/General Experience:**
- 3 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

---

IT Auditor

**GSA Rate:** $100.24

**Functional Responsibility:** Establish and/or review audit objectives and devise audit plans. Follow general audit plans and previous audit reports where available, and recommend guidelines for data collection and reporting procedures. Interview organizational staff and examine records to gather, analyze and evaluate data concerning the effectiveness of controls. Determine accuracy of reports and efficiency and security of operations and provide audit reports to document findings and recommendations. Provide support by researching and implementing applicable computer programs for company use to conduct audits. As appropriate, develop, devise, write, and test computer programs required to obtain information needed to perform an appropriate audit. Where new or untested procedures are involved, devise controls to prevent inaccurate calculations or data loss, and ensure discovery of errors.

**Minimum/General Experience:**
- 3 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Systems Engineer

GSA Rate: $116.54

**Functional Responsibility:** Ability to work independently with minimal technical oversight. Responsible for leading or participating in system concept design, integration and troubleshooting of subsystems and interpretation of operational requirements. Collects, interprets and documents system requirements. Leads or participates in component, subsystem and/or system concept design verifying key design parameters and evaluating design options with appropriate experimentation; possibly analyzes designs for system interactions. Performs trade-offs and feasibility studies. Well-versed in the concepts of formalized system or software engineering principles and processes (e.g. the Software Development Lifecycle) as it pertains to developing the appropriate artifacts and system documentation to effectively apply technology solutions through a systems engineering process. Generally has experience in at least one of the following: System analysis, generation of requirements and interface specifications; System engineering reviews and management of engineering issues and issues resolution; Subsystem design, development, and testing; Preparation of System Integration and Test planning activity; Producing Integration and Acceptance Test Plans/Procedures; Developing Test Specifications.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Network Engineer

GSA Rate: $108.41

**Functional Responsibility:** Ability to work independently with minimal technical oversight. Provide network systems engineering guidance and support. Manage network performance and maintain network security. Develop network topology designs, IP network routing architectures, and/or advise on technology investments and migration strategies. Assess performance and security impacts. Troubleshoots network problems and performs hands-on test and evaluation of network and application scenarios. Support development/analyses of network designs and protocols to include prototyping and experimentation. Participate in all aspects of network support to include installing, supporting and maintaining new server hardware and software infrastructure, managing email, anti-spam, and virus protection. Generally has experience in one or more of the following: Thorough understanding of routing, transport, QoS, security, and performance concerns for communications networks; Cisco or Juniper router and switch configuration for LAN/WAN environments; Firewall and IDS device configuration experience; Cryptographic devices/systems; HAIPE/IPSec performance analysis; Network security; MPLS architecture; C/C++ or JAVA programming; VoIP protocols and networks, mobile ad-hoc networking, analyzing network performance using OPNET, and IPv6.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Technology Engineer  

GSA Rate: $118.76

Functional Responsibility: Ability to work independently with minimal technical oversight. Responsible for providing analysis, consultation, recommendations, and/or developing approaches to inserting technology solutions in support of organizational requirements and mission goals. Lead or participate in the development of technology solutions and architectures to leverage industry best practices in support of customer needs, compliance requirements, and/or government mandates or initiatives. Work closely with engineering teams in the concept design, development, implementation, and/or ongoing support of an IT system or subsystem. Provides mentorship and guidance to engineering teams supporting a technical solution. Proactively troubleshoots and provides recommendations to improving all aspects of a technical solution (e.g., performance, cost effectiveness, mission support, security). Performs market and industry research to stay current on trends and emerging technologies and identifies areas to integrate improvements where applicable. Strong written and communication skills.

Minimum/General Experience:
- 5 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field

Engineer  

GSA Rate: $118.76

Functional Responsibility: Ability to work both independently and within an integrated project team. Responsible for contributing to concept design, development, implementation, and/or ongoing support of an IT system, subsystem, or component. Translates business requirements into a technical solution to meet those requirements. Participates as part of engineering team supporting a technical solution. Proactively troubleshoots and provides recommendations to improving all aspects of a technical solution (e.g., performance, cost effectiveness, mission support, security). Stays current on industry trends and emerging technologies and identifies areas to integrate improvements where applicable.

Minimum/General Experience:
- 5 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field

Senior Engineer  

GSA Rate: $132.46

Functional Responsibility: Ability to manage a team and provide technical oversight. Responsible for leading in the concept design, development, implementation, and/or ongoing support of an IT system, subsystem, or component. Translates business requirements into a technical solution to meet those requirements. Provides mentorship and guidance to engineering team supporting a technical solution. Proactively troubleshoots and provides recommendations to improving all aspects of a technical solution (e.g., performance, cost effectiveness, mission support, security). Stays current on industry trends and emerging technologies and identifies areas to integrate improvements where applicable. Strong written and communication skills.

Minimum/General Experience:
- 8 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field
Consultant

**Functional Responsibility:** Ability to work independently with minimal oversight. Demonstrates understanding of the relationship and interaction between business and information technology. Provides consultation and guidance in identifying practical and effective solutions to support business needs. Generalized experience in project management, all aspects of system or software development, and industry research on new technologies. Possesses working knowledge of government regulations and mandates. Often provides advice within a specific field of expertise. Develop white papers, position papers or functional/technical products as required. Readily able to provide presentations on technical solutions, industry trends, etc., as well as participate in Q&A sessions with customer community to educate people on particular field of expertise. Strong written and communication skills.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Senior Consultant

**Functional Responsibility:** Ability to work independently with minimal oversight. Demonstrates deep understanding of the relationship and interaction between business and information technology. Provides expert consultation and guidance in identifying practical and effective solutions to support business needs. Generalized experience in project management/leadership, all aspects of system or software development, and industry research on new technologies. Well-versed in government regulations and mandates. Often provides expert advice within a specific field of expertise. Develop white papers, position papers or functional/technical products as required. Readily able to provide presentations on technical solutions, industry trends, etc., as well as participate in Q&A sessions with customer community to educate people on particular field of expertise. Strong written and communication skills.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field

Systems Architect

**Functional Responsibility:** Ability to work independently with minimal technical oversight. Provide input on mapping an organization’s business strategy into an information technology systems architecture to support that strategy. Ensure that technology objectives are aligned to business goals. Participate in the development and review of the conceptual architecture and high level design of major projects and system enhancements. Provide technology direction and promote system and architecture design methods and tools that enable the integration of disparate systems.

Generally has experience in one or more of the following: designing n-tier applications for both internal and external business environments, to possibly include service-oriented architecture (SOA) deployments; A significant understanding and knowledge of commonly used concepts, practices and procedures within the system or software development field is required. Strong working knowledge of application architecture, design patterns, and/or development methodologies/frameworks. Ability to communicate effectively and work in a team environment.

**Minimum/General Experience:**
- 5 years IA/IS experience

**Minimum Education:**
- BS degree in Computer Science, Information Systems, Engineering, or related field
Senior Systems Architect

GSA Rate: $137.04

Functional Responsibility: Ability to work independently with minimal technical oversight. Provide input and guidance on mapping an organization’s business strategy into an information technology systems architecture to support that strategy. Ensure that technology objectives are aligned to business goals. Participate in the development and review of the conceptual architecture and high level design of major projects and system enhancements. Provide input on conceptual models, strategies, and long term technical directions of an organizations IT portfolio. Influence technology direction and promote system and architecture design methods and tools that enable the integration of disparate hardware and software systems.

Generally has experience in one or more of the following: Experience and aptitude in learning new technologies, researching, documenting, analyzing, and problem solving. Experience in designing n-tier applications for both internal and external business environments, to possibly include service-oriented architecture (SOA) deployments. A significant understanding and knowledge of commonly used concepts, practices and procedures within the system or software development field is required. Strong working knowledge of application architecture, design patterns, and development methodologies/frameworks. Ability to communicate effectively and work in a team environment.

Minimum/General Experience:
- 8 years IA/IS experience

Minimum Education:
- BS degree in Computer Science, Information Systems, Engineering, or related field