



**GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST**

Online access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order is available through GSA Advantage!®, a menu-driven database system. The Internet address for GSA Advantage!® is <http://www.gsaadvantage.gov>

Schedule Title: MULTIPLE AWARD SCHEDULE (MAS)

FSC Group: LARGE CATEGORY: INFORMATION TECHNOLOGY; SUBCATEGORY: IT SERVICES

PSC Class: D399

Contract Number: 47QTC A18D00H7

Contract Period: August 3, 2023 through August 2, 2028

Business Size: Small

Current through Refresh 0015

For more information on ordering from Federal Supply Schedules click on FSS Schedules at: <http://fss.gsa.gov/>.



Crystal Management, LLC

3400 Stately Oaks Lane

Duluth, Georgia 30097

Phone: 703-582-4234

Fax: 800-211-8729

www.cmitmanage.com

Contract Administration: John Lehman, President

Email: jlehman@cmitmanage.com

Table of Contents

Customer Information	3
Information Technology (IT) Professional Services (SIN 54151S) - Terms and Conditions.....	7
Information Technology (IT) Professional Services (SIN 54151S) - Price List.....	11
Information Technology (IT) Professional Services (SIN 54151S) - Labor Category Descriptions	12
Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) - Terms and Conditions	27
Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) - Price List.....	36
Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) – Labor Category Descriptions	36

Customer Information

1. Awarded Special Item Numbers (SINs)

Special Item Number (SIN)	Description
54151HACS	Penetration Testing - 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.
54151HACS	Incident Response - 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
54151HACS	Cyber Hunt - Cyber hunt activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities
54151HACS	Risk and Vulnerability Assessments - Risk and vulnerability assessments conduct assessments of 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. At a minimum, offerors who would like to be considered for this SIN must offer the following services: Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessment.
54151HACS	High Value Asset (HVA) Assessments – 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. See the section on RVA for details on those services. 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

	<p>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.</p>
54151S	<p>Information Technology Professional Services – This SIN includes resources and facilities management, database planning and design, systems analysis and design, network services, programming, conversion and implementation support, network services project management, data/records management, and other services relevant to 29CFR541.400</p>

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. N/A

1c. Refer to Labor Category Descriptions sections for labor categories, education and experience requirements, and functional responsibilities. Labor Category Descriptions for HACS on pages 36-43 and Information Technology Professional Services on pages 11-26.

2. Maximum Order: \$500,000

3. Minimum Order: \$100

4. Geographic Coverage (delivery area): Worldwide

5. Point(s) of Production: Duluth, GA

6. Discount from List Prices or Statement of Net Price: Prices shown are GSA net prices, and the IFF is included.

7. Quantity Discount: None

8. Prompt Payment Terms: Net 30

9. Foreign Items: Not applicable

10a. Time of Delivery: Negotiated at Task Order Level

10b. Expedited Delivery: Not available

10c. Overnight and 2-Day Delivery: Not applicable

10d. Urgent Requirements: Agencies can contact the Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

11. F.O.B. Point: Destination

Note: All travel required in the performance of this contract and orders placed hereunder must comply with the Federal Travel Regulations (FTR) or Joint Travel Regulations (JTR), 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. The contractor shall not add the Industrial Funding Fee onto travel costs.

12a. Ordering Address: Same as Contractor's address

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

13. Payment Address: Same as Contractor's address

14. Warranty Provisions: Not applicable

15. Export Packing Charges: Not applicable

16. Terms and Conditions of Rental, Maintenance, and Repair: Not applicable

17. Terms and Conditions of Installation: Not applicable

18a. Terms and Conditions of Repair Parts: Not applicable

18b. Terms and Conditions for Any Other Services: Not applicable

19. List of Service and Distribution Points: Not applicable

20. List of Participating Dealers: Not applicable

21. Preventive Maintenance: Not applicable

22a. Special Attributes (e.g., environmental attributes): Not applicable

22b. Section 508 Compliance: Not applicable

23. Data Universal Number System (DUNS): 624050782

SAM Unique Entity ID (UEI): MC9MJ8UWBFK6

24. Notification Regarding Registration in System for Award Management (SAM) Database:
Registered, registration valid to September 19, 2023.

Information Technology (IT) Professional Services (SIN 54151S) - Terms and Conditions

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

- 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

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4

CONTRACT TERMS AND CONDITIONS - COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I - OCT 2008) (DEVIATION I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

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” refer 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

Information Technology (IT) Professional Services (SIN 54151S) - Price List

Labor Category	GSA Price (including IFF)					
	Base Period Year 5 Rate 8/3/2022- 8/2/2023	Opt 1 Period - Year 6 Rate 8/3/2023- 8/2/2024	Opt 1 Period - Year 7 Rate 8/3/2024- 8/2/2025	Opt 1 Period - Year 8 Rate 8/3/2025- 8/2/2026	Opt 1 Period - Year 9 Rate 8/3/2026- 8/2/2027	Opt 1 Period - Year 10 Rate 8/3/2027- 8/2/2028
Applications Support Specialist	\$ 108.27	\$ 111.52	\$ 114.86	\$ 118.31	\$ 121.85	\$ 125.51
Business Analyst	\$ 130.80	\$ 134.72	\$ 138.76	\$ 142.92	\$ 147.21	\$ 151.63
Communications Specialist	\$ 113.05	\$ 116.44	\$ 119.94	\$ 123.54	\$ 127.24	\$ 131.06
Data Analyst	\$ 111.23	\$ 114.57	\$ 118.01	\$ 121.54	\$ 125.19	\$ 128.95
Database Administrator	\$ 104.37	\$ 107.51	\$ 110.73	\$ 114.06	\$ 117.48	\$ 121.01
Help Desk Representative	\$ 72.65	\$ 74.83	\$ 77.08	\$ 79.40	\$ 81.77	\$ 84.22
Infrastructure Engineer	\$ 120.58	\$ 124.20	\$ 127.93	\$ 131.77	\$ 135.72	\$ 139.79
Network Administrator	\$ 116.57	\$ 120.07	\$ 123.68	\$ 127.39	\$ 131.20	\$ 135.14
Network Engineer	\$ 138.15	\$ 142.29	\$ 146.56	\$ 150.95	\$ 155.48	\$ 160.14
Project Administrator	\$ 96.75	\$ 99.65	\$ 102.64	\$ 105.72	\$ 108.90	\$ 112.16
Project Controls Engineer	\$ 133.56	\$ 137.57	\$ 141.70	\$ 145.95	\$ 150.34	\$ 154.85
Project Manager III	\$ 170.51	\$ 175.63	\$ 180.90	\$ 186.33	\$ 191.92	\$ 197.67
Project Manager II	\$ 142.88	\$ 147.16	\$ 151.58	\$ 156.12	\$ 160.81	\$ 165.63

Labor Category	GSA Price (including IFF)					
	Base Period Year 5 Rate 8/3/2022- 8/2/2023	Opt 1 Period - Year 6 Rate 8/3/2023- 8/2/2024	Opt 1 Period - Year 7 Rate 8/3/2024- 8/2/2025	Opt 1 Period - Year 8 Rate 8/3/2025- 8/2/2026	Opt 1 Period - Year 9 Rate 8/3/2026- 8/2/2027	Opt 1 Period - Year 10 Rate 8/3/2027- 8/2/2028
QA Inspector	\$ 85.31	\$ 87.87	\$ 90.51	\$ 93.22	\$ 96.02	\$ 98.90
Quality Assurance Analyst	\$ 117.88	\$ 121.42	\$ 125.07	\$ 128.82	\$ 132.69	\$ 136.66
Security Analyst	\$ 116.91	\$ 120.41	\$ 124.03	\$ 127.75	\$ 131.58	\$ 135.53
Security Engineer	\$ 137.56	\$ 141.69	\$ 145.94	\$ 150.33	\$ 154.84	\$ 159.49
Security Specialist	\$ 122.85	\$ 126.54	\$ 130.34	\$ 134.25	\$ 138.28	\$ 142.43
Software Developer	\$ 147.18	\$ 151.60	\$ 156.14	\$ 160.83	\$ 165.65	\$ 170.62
Subject Matter Expert III	\$ 187.17	\$ 192.79	\$ 198.57	\$ 204.52	\$ 210.66	\$ 216.98
Subject Matter Expert II	\$ 162.95	\$ 167.84	\$ 172.88	\$ 178.07	\$ 183.41	\$ 188.91
Subject Matter Expert I	\$ 133.32	\$ 137.32	\$ 141.44	\$ 145.68	\$ 150.06	\$ 154.56
Systems Administrator	\$ 120.19	\$ 123.80	\$ 127.52	\$ 131.35	\$ 135.28	\$ 139.35
Systems Engineer	\$ 147.82	\$ 152.25	\$ 156.82	\$ 161.52	\$ 166.37	\$ 171.36
Technical Training Instructor	\$ 103.96	\$ 107.08	\$ 110.30	\$ 113.60	\$ 117.01	\$ 120.51

Information Technology (IT) Professional Services (SIN 54151S) - Labor Category Descriptions

The descriptions provided include representative job duties and responsibilities, as well as typical education and work experience associated with each labor category type. The nominal academic credentials and years of experience required at each level is also provided.

Education may be substituted for experience, and conversely, experience may be substituted for education in accordance with the following guidelines:

Academic Degree	Equivalent Experience*
Associates	1 year relevant experience
Bachelors	2 years relevant experience
Masters and higher	5 years relevant experience

Applications Support Specialist

Minimum Education: Bachelor’s Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Coordinates the planning, design, and installation of systems and software applications in an enterprise environment, using knowledge of engineering and programming as well as sophisticated instruments and computers. Analyzes functional business applications and design specifications for functional activities. Develops, runs tests, and maintains current computer aided programs that provide instructions computers must follow to perform their function. Develops block diagrams and logic flow charts. Translates detailed design into computer software. Prepares required documentation, including both program-level and user-level documentation. Enhances software to reduce operating time or improve efficiency. Creates, compiles, delivers, and sustains quality and consistent content for websites based on management priorities, policy directives, and goals. Works with graphic designers and other members of a project team to develop the site concept, interface design, and architecture of the website.

Business Analyst

Minimum Education: Bachelor’s Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Analyzes company functions, processes, and activities to improve computer- based business applications and systems for the most effective use of money, materials, equipment, and people. Utilizes available computer systems resources and personnel to carry out analysis to support management's quest for performance improvement. Reviews and analyzes information, forecasts, methods, schedules, systems, processes, and procedures. Recommends alternative solutions to management as to courses of action that best meet the organization's goals. Applies the use of process improvement, reengineering methodologies, and

internet-related methodologies and principles to conduct process modernization projects. May devise and design business process requirements for all IT- related business, financial, and operations systems critical to core organizational functions. This includes researching and analyzing data in support of business functions, process knowledge, and systems requirements. Provides support in the areas of budget, billing, reporting, and financial management for IT initiatives. Assists in applying sound accounting and data processing principles. Integrates government financial business practices. Identifies potential problems and solutions through analysis and recommends solutions.

Communications Specialist

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Evaluates communication hardware and software, troubleshoots LAN/MAN/WAN and other network related problems, and provides technical expertise for performance, network management and configuration of networks. Participates in engineering activities of an organization's information systems. Plans, designs, develops, evaluates, tests, and integrates an organization's systems infrastructure, including the implementation and design of hardware and software. Performs general LAN/MAN/WAN administration, provides technical support in the integration and test of complex large-scale computer integrated networks. Responsible for high-level analysis, evaluation, design, integration, documentation, and implementation of applications for Information Technology (IT) and Command, Control, Computer, Communications and Intelligence (C4I) projects. Creates, starts implementation, installs, repairs, and maintains data, voice, and network communications systems, using hand tools and software and hardware testing instruments and techniques. Implements recommended equipment modifications and enhancements in accordance with user request and business objectives. Install, maintain, and repair cable systems. Test and troubleshoot issues with network communication. Pull, route, or label CAT5 or CAT6 cable. Install various passive infrastructure elements, including cable racks, j-hooks, innerduct, and other related structures. Communicate and collaborate with other members of the field service team to resolve complex issues.

Data Analyst

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Performs IT systems-based identification, query, transform, integration, and analysis of structured and unstructured client data using software products and computer-oriented tools. Manipulate and convert data for customer and Commercial of the Shelf (COTS) IT platforms to perform business intelligence (BI), link analysis, and data fusion of government and private data sets to transform data into knowledge. Develop tables, graphs, and dashboards to communicate the results of data analysis activities to provide effective decision support for customers. Data analysis activities may require specialized skills or background including, for instance, cyber security experience. Specific responsibilities may include: data entry, data integrity checks, and report development and analysis. Designs data architectures to support present and future requirements and interfaces. Uses design tools and techniques to establish logical and physical data models. Designs and implements databases, data warehouses, data lakes, or other types of data repositories. Plans technical functionality (e.g., scalability, security, performance, data recovery, reliability). Ensures data systems are compatible and compliant with relevant standards. Provides support in the areas of budget, billing, reporting, and financial management for IT initiatives.

Database Administrator

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Design, install, monitor, operate, maintain, and performance tune production databases while ensuring high levels of data availability. This individual is also responsible for developing, implementing, and overseeing database policies and procedures to ensure the integrity and availability of databases and their accompanying software. Provide system analysis, database development support to include the integration, conversion and migration of data from one system to another.

Help Desk Representative

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 2 years of experience

Functional Responsibility: Provide tier 1 general IT technology or network management services, such as answer questions in person, via phone or email on all company supported systems and applications. Troubleshoot basic computer problems and create trouble tickets in

the required system. Determine source of computer problems (hardware, software, user access, etc.) and escalate to the appropriate support team. Serve as liaison between users and the support teams to resolve issues. May be required to coordinate activities of employees engaged in receiving requests for assistance and interpreting problems, providing assistance, problem-solving support, and advising computer user related to hardware, software, and systems. Aids User Support Analyst in solving non-routine software, hardware, and procedure problems. Escalates problems and issues to management and the client on a timely basis.

Infrastructure Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Plans, directs, designs and coordinates activities concerned with the IT infrastructure, for example - security, data center support, active and passive network components as well as IT facility operations. This may include designing, planning and laying and repairing cables. Responsible for planning, preparing and/or reviewing/validating drawings for construction of new, removal or rearrangement of existing, overhead or underground lines, cables and conduits to obtain optimum and economical utilization of communications facilities. Prepares and/or reviews and validates construction and installation drawings, estimates equipment, labor and material costs. Initiates and/or reviews and validates work authorization requests and submission of substantiating drawings and documents to management for approval. Orders and/or reviews and validates ordering of materials and equipment required and directs and/or oversees/performs quality assurance surveillance of work activities to ensure conformance with engineering specifications and work authorization. Creates, starts implementation, installs, repairs, and maintains data, voice, and network systems, using hand tools and software and hardware testing instruments and techniques. Implements recommended equipment modifications and enhancements in accordance with user request and business objectives. Oversees IT facilities planning, ensuring that the facility complies with all applicable building codes; and ensures compliance with the engineering limitations of structures within the facility. Determines feasibility of designing or modifying new data center equipment or facilities considering costs, available space, time limitations, company planning, and other technical and economic factors, utilizing professional engineering theory and practices. Plans and administers research and development activities concerned with design, construction, and production of data center facilities and systems. Provide electrical, mechanical, plumbing or fire protection data center design service to internal and external project teams. Plans and performs security

engineering research, design, development, integration and other assignments in conformance with system design, engineering, and customer specifications.

Network Administrator

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Provides network management services for LAN, MAN or WAN networks by managing, administering, troubleshooting and maintaining hubs, servers, switches and routers. Utilizes knowledge and understanding of both networking and telecommunications theory and practice to troubleshoot, configure and resolve network related problems. Maintains network performance by performing network monitoring and analysis, and performance tuning; troubleshooting network problems; escalating problems to vendor. Recommend configuration management solutions that effectively meet customer requirements. Plan and coordinate system configuration activities for timely completion. Maintain configuration management documentations for reference purposes. Analyze and resolve configuration problems in a timely fashion. Communicate configuration discrepancies to Management for immediate resolutions.

Network Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Analyze requirements and engineer network solutions for federal clients. Provide tier 2 and 3 network management troubleshooting support. Facilitate working group meetings to capture technical and business requirements. Participate in vendor meetings to evaluate and validate product features and functionality. Assist with coordinating implementation activities and facilitating effective communications between key stakeholders and the implementation teams. Facilitate weekly technical working group meetings to discuss and resolve implementation issues. Work within several IT disciplines, including Internet and computing technologies, networking and telecommunications, and radio. Some engineers concentrate on applying technical knowledge across several domains, i.e. data, VoIP and converged networks. The technical aspect of the role includes using specialist knowledge to design and deliver solutions, as well as providing technical guidance to others within the employing organization.

Project Administrator

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Performs general IT services, such as basic analysis, development and review of program or functional areas, as required. Researches, writes, edits, and proofreads technical data for use in documents or sections of documents such as manuals, procedures, specifications, special reports, and any other customer deliverables and documents.

Knowledgeable in IT Acquisition process and its milestones, analyzing a variety of source documentation, and the creation of acquisition documentation. Formulates and coordinates procurement proposals. Provides analytical management assistance by helping plan, conduct surveys and studies, and special projects. The position performs responsible administrative and budget research and analyses and provides recommendations. Supports an organization or department by performing project support and administrative services. Prepares various reports and deliverables. Provides administrative support such as writing, proofreading, editing of word processing and other computer-based documents, integration of various sources into a cohesive product which may be delivered as computer-based magnetic media, and preparation of graphical and narrative presentation material. Provides assistance with maintaining personnel and other files; prepares correspondence, schedules and coordinates travel. Coordinates schedules to facilitate completion of proposals, contract deliverables, task order review, briefings/presentations.

Project Controls Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Develops and implements standard cost and schedule programs, processes, and practices on specific IT or network management services projects, including creation of complex Integrated Master Schedules. Develops the overall status reporting on the financial aspects and the schedules associated with these projects. Utilizes knowledge of scope coordination and analysis, work package review, project schedule development, work breakdown structures, cost engineering, critical path analysis, contractor coordination and management, accountancy principals, practices, and concepts, integrated cost and scheduling, budget development, cost accounting and forecasting, variance analysis, performance reporting, contingency planning, root cause analysis, and contract commercial provisions and interpretations. Identifies trends and deviations in cost performance against budget alerting Project Management to potential problem areas.

Project Manager III

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 15 years of experience

Functional Responsibility: Assumes responsibility for day-to-day project management of all activities and functions in a designated large, complex project which involves facility O&M, system analysis and development, programming, security and network management services, security or other IT related services. This includes developing, implementing and evaluating program policies, procedures and standards; determining program service levels and enhancements; developing and monitoring program budgets; providing technical advice and/or supervision to staff, other departments, the public and other agencies, and performs related work as required. Responsible for client relationship and all deliverable and contractual performance. Organizes and manages resources in such a way that these resources deliver all the work required to complete a project within a defined scope, time, and cost constraints. Manages the daily activities of the project and meets with project stakeholders; takes lead role and works with project stakeholders to develop: WBS and Schedule, Project Standards, Change Control Plan, Resource and Staffing Plan, Budget Plan, Risk Management Plan, and Communication Plan, as well as Review Project Methodology and approach.

Project Manager II

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Assumes responsibility for day-to-day project management of all activities and functions in a designated medium-sized projects which involves facility O&M, system analysis and development, programming, security and network management services, security or other IT related services. Organizes and manages resources in such a way that these resources deliver all the work required to complete a medium sized project within a defined scope, time, and cost constraints. Manages the daily activities of the project and meets with project stakeholders; takes lead role and works with project stakeholders to develop: WBS and Schedule, Project Standards, Change Control Plan, Resource and Staffing Plan, Budget Plan, Risk Management Plan, and Communication Plan, as well as Review Project Methodology and approach.

Project Manager I

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 2 years of experience

Functional Responsibility: Assumes responsibility for day-to-day project management of all activities and functions in designated small projects which involves facility O&M, system analysis and development, programming, security and network management services, security or other IT related services. Organizes and manages resources in such a way that these resources deliver all the work required to complete a small project within a defined scope, time, and cost constraints. Manages the daily activities of the project and meets with project stakeholders; takes lead role and works with project stakeholders to develop: WBS and Schedule, Project Standards, Change Control Plan, Resource and Staffing Plan, Budget Plan, Risk Management Plan, and Communication Plan, as well as Review Project Methodology and approach.

QA Inspector

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Ensures by inspection that data, network, database and other similar IT systems that are designed, programmed, installed, implemented, converted meet quality requirements. Supports the technical relationship with customers on existing products and services. Works directly with customers and internal resources in obtaining requested information, problem resolution, and identifying opportunities for continuous improvement. Performs internal supplemental audits of a technical discipline to verify that results and records (e.g., equipment, training files) are in conformance to applicable SOP, client and regulatory requirements. Performs protocol, data, report, and inspections in a technical discipline to verify conformance to applicable SOP requirements. Performs system testing activities for a particular project or subset of a larger project under supervision of more experienced test personnel.

Quality Assurance Analyst

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Ensures through the implementation of a quality assurance plan that data, network, database and other similar IT systems that are designed, programmed, installed, implemented, converted meet quality assurance requirements. Works directly with customers and internal resources in obtaining requested information, problem resolution, and

identifying opportunities for improvement. Performs internal supplemental audits of a technical discipline to verify that facility records (e.g., equipment, training files) are in conformance to applicable SOP and regulatory requirements. Provides quality assurance and control services. Performs protocol, data, report, and inspections in a technical discipline to verify conformance to applicable SOP requirements. Oversees the development and implementation of all quality control methodologies to ensure compliance with all applicable standards and guidelines directed by the customer. Conducts the review of program documentation to assure ordering activity standards are met. Prepares milestone status reports. Performs application and system testing activities for a project or subset of a larger project under supervision of more experienced test personnel.

Security Analyst

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Investigates and contributes to complex computer security incident response events on networks. Leverages advanced tools to identify and mitigate malicious activity, ranging from malware to potential interactive intrusions. Analyzes computer systems, network traffic, vulnerability scans, penetration tests for signs of infection and compromise, correlate data and take corrective action. Characterizes suspicious binaries and be able identify traits. Identify potential malicious activity from memory dumps, logs, and packet captures. Interact and assist other investigative teams on time sensitive, critical investigations. Act as a security engineering expert on information security related issues pertaining to malware analysis, phishing assessment and incident response. Analyze security and network defense policies and configurations (i.e. access control lists and firewall settings) to ensure they are in compliance with regulations and client directives.

Security Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Under direction, designs, deploys and maintains enterprise computer network and security defense capabilities from the enterprise down to the end point, to include the selection of cost effective security controls to mitigate risks. Knowledgeable in information assurance software, hardware, or both. Supports the capture of relevant IT requirements and assists team leads and project managers with information assurance/security

architecture and designs. Once deployed, operates, maintains and tunes security systems across network, data center, cloud, and at the application layer as needed. Reports performance issues to senior management. Assists security analysts and specialists with advanced security problems and issues. May provide technical leadership in analyzing security and network defense policies and configurations (i.e. access control lists and firewall settings) to ensure they are in compliance with regulations and client directives. Provides engineering assistance in the identification of IT vulnerabilities for client's systems.

Security Specialist

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: 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, phishing, 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. Collects intrusion artifacts and responds to incidents, investigates violations, correlates data and recommends enhancements to plug potential security gaps. Performs risk analyses which also includes risk assessment, identifies, investigates, analyzes, and remediates information security events to ensure enterprise integrity against technical and physical risks. Conducts quality management reviews to evaluate the effectiveness of security controls. This position reports on the controls effectiveness for mitigating exposure to identified risks. Communicates security issues and control gaps through security governance processes. This position implements and integrates risk management procedures across the enterprise. Participates in the development and maintenance of business continuity planning, data, systems, and network security for systems & controls related to their job duties. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines.

Software Developer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Provide programming services such as develops, runs tests, and maintains computer applications that provide instructions computers must follow to perform their function. Creates programs according to specifications, which may be provided by other software developers or support team. Updates, repairs, modifies, and expands existing computer programs. Participates in the design, coding, testing, support and debugging of new software or significant enhancements to new and/or existing software applications. Perform coding, debugging and testing to define the integration between proposed development projects and existing systems. Considers and researches emerging technologies to improve current applications, architectures and processes. Design, develops, and implements customized solutions for various systems. Also provides post deployment support for all custom applications and implementations provided to the government. Provides functional and empirical analysis related to the design, development and implementation of software and software operating systems, including, but not limited to, utility software, development software, and diagnostic software. Participates in the development of test strategies, devices and systems.

Subject Matter Expert (SME) III

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 15 years of experience

Functional Responsibility: Performs as a consultant in a highly specialized, leading edge information technologies and methodologies related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides highly technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME III understands, articulates and implements best practices related to their area of expertise. The SME may lead a work-group with the need for specialized knowledge. The SME III provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business and technical solutions.

Subject Matter Expert (SME) II

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Under general guidance, performs as a consultant in a highly specialized, leading edge information technologies and methodologies related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides highly technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME II understands, articulates and implements best practices related to their area of expertise. The SME II provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business and technical solutions.

Subject Matter Expert (SME) I

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 2 years of experience

Functional Responsibility: Under specific direction, performs as a consultant in highly specialized, leading edge information technologies and methodologies related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME I understands, articulates and implements best practices related to their area of expertise. Working with a team, the SME I provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement solutions.

Systems Administrator

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Installs, configures, optimizes for performance and monitors systems and related applications. Performs a variety of maintenance, evaluation, installation, and training tasks to ensure system performance meets company and user requirements. Analyzes and solves computer problems, and assures technology meets the needs of the organization. Develops and implements system studies to assist organization to realize maximum benefit from investments in equipment, personnel, and business processes. Analyzes user interfaces, maintain hardware and software performance tuning, analyze workload and computer usage, maintain interfaces with outside systems, analyze downtimes, analyze proposed system modifications, upgrades and new COTS. Analyzes the problem and the information to be processed. Defines the problem, and develops system requirements and program specifications, from which programmers prepare detailed flow charts, programs, and tests.

Systems Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Participates in complex engineering activities of an organization's information systems. Plans, designs, develops, evaluates, tests, and integrates an organization's systems infrastructure, including the implementation and design of hardware and software. Responsible for high-level systems analysis, evaluation, design, integration, documentation, and implementation of very complex applications for Information Technology (IT) and Command, Control, Computer, Communications and Intelligence (C4I) projects. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance phases. Applies higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solution. Possesses in-depth knowledge of contemporary systems engineering concepts, practices, and procedures. Applies advanced concepts, theories and principles of computing solutions for scalable virtual activities within an enterprise or a large federal agency. Responsible for engineering, implementing, optimizing and administering cloud solutions, infrastructures and platforms. Provides recommendations for future technologies and capacity growth.

Technical Training Instructor

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Organizes and conducts training and educational programs for information systems (technical) or user (non-technical) personnel. Develops and provides IT and end user training on computer hardware, systems and application software. Conducts the research necessary to develop and revise training courses and prepares appropriate training catalogs. Confers with management and staff or technical training coordinator to determine training objectives. Prepares all instructor materials (course outline, background material, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms).

Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) - Terms and Conditions

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- **Federal Acquisition Regulation (FAR) Part 52.204-21**
- **OMB Memorandum M-06-19** - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- **OMB Memorandum M -07-16** - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- **OMB Memorandum M-16-03** - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- **OMB Memorandum M-16-04** – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- **The Cybersecurity National Action Plan (CNAP)**
- **NIST SP 800-14** - Generally Accepted Principles and Practices for Securing Information Technology Systems
- **NIST SP 800-27A** - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- **NIST SP 800-30** - Guide for Conducting Risk Assessments
- **NIST SP 800-35** - Guide to Information Technology Security Services
- **NIST SP 800-37** - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- **NIST SP 800-39** - Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST SP 800-44** - Guidelines on Securing Public Web Servers
- **NIST SP 800-48** - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-61** - Computer Security Incident Handling Guide

- **NIST SP 800-64** - Security Considerations in the System Development Life Cycle
- **NIST SP 800-82** - Guide to Industrial Control Systems (ICS) Security
- **NIST SP 800-86** - Guide to Integrating Forensic Techniques into Incident Response
- **NIST SP 800-115** - Technical Guide to Information Security Testing and Assessment
- **NIST SP 800-128** - Guide for Security-Focused Configuration Management of Information Systems
- **NIST SP 800-137** - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- **NIST SP 800-153** - Guidelines for Securing Wireless Local Area Networks (WLANs)
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE

- a. The labor categories, prices, terms, and conditions stated under Special Item Numbers 54151HACS apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.
- b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only.



- c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
- d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
- e. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. ORDER

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

3. PERFORMANCE OF SERVICES



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

4. INSPECTION OF SERVICES

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

5. RESPONSIBILITIES OF THE CONTRACTOR



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

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

9. INVOICES



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

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

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

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

- a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item 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 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).



Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) - Price List

Labor Category	GSA Price (including IFF)					
	Base Period - Year 5 Rate 8/3/2022- 8/2/2023	Opt 1 Period - Year 6 Rate 8/3/2023- 8/2/2024	Opt 1 Period - Year 7 Rate 8/3/2024- 8/2/2025	Opt 1 Period - Year 8 Rate 8/3/2025- 8/2/2026	Opt 1 Period - Year 9 Rate 8/3/2026- 8/2/2027	Opt 1 Period - Year 10 Rate 8/3/2027- 8/2/2028
Cyber Security Analyst	\$ 116.91	\$ 120.41	\$ 124.03	\$ 127.75	\$ 131.58	\$ 135.53
Cyber Security Engineer	\$ 137.56	\$ 141.69	\$ 145.94	\$ 150.33	\$ 154.84	\$ 159.49
Cyber Security Specialist	\$ 122.85	\$ 126.54	\$ 130.34	\$ 134.25	\$ 138.28	\$ 142.43
Cyber Subject Matter Expert III	\$ 187.17	\$ 192.79	\$ 198.57	\$ 204.52	\$ 210.66	\$ 216.98
Cyber Subject Matter Expert II	\$ 162.95	\$ 167.84	\$ 172.88	\$ 178.07	\$ 183.41	\$ 188.91

Highly Adaptive Cybersecurity Services (HACS) (SIN 54151HACS) – Labor Category Descriptions



The descriptions provided include representative job duties and responsibilities, as well as typical education and work experience associated with each labor category type. The nominal academic credentials and years of experience required at each level is also provided.

Education may be substituted for experience, and conversely, experience may be substituted for education in accordance with the following guidelines:

Academic Degree	Equivalent Experience*
Associates	1 year relevant experience
Bachelors	2 years relevant experience
Masters and higher	5 years relevant experience

Cyber Security Analyst

Minimum Education: Bachelor’s Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Investigates and contributes to complex computer security incident response events on networks. Leverages advanced tools to identify and mitigate malicious activity, ranging from malware to potential interactive intrusions. Analyzes computer systems, network traffic, vulnerability scans, penetration tests for signs of infection and compromise, correlate data and take corrective action.

Characterizes suspicious binaries and be able identify traits. Identify potential malicious activity from memory dumps, logs, and packet captures. Interact and assist other investigative teams on time sensitive, critical investigations. Act as a security engineering expert on information security related issues pertaining to malware analysis, phishing assessment and incident response. Analyze security and network defense policies and configurations (i.e. access control lists and firewall settings) to ensure they are in compliance with regulations and client directives. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Certified Ethical Hacker (CEH) is preferred but not required.*

Cyber Security Engineer

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: Under direction, designs, deploys and maintains enterprise computer network and security defense capabilities from the enterprise down to the end point, to include the selection of cost effective security controls to mitigate risks. Knowledgeable in information assurance software, hardware, or both. Supports the capture of relevant IT requirements and assists team leads and project managers with information assurance/security architecture and designs. Once deployed, operates, maintains and tunes security systems across network, data center, cloud, and at the

application layer as needed. Reports performance issues to senior management. Assists security analysts and specialists with advanced security problems and issues. May provide technical leadership in analyzing security and network defense policies and configurations (i.e. access control lists and firewall settings) to ensure they are in compliance with regulations and client directives. Provides engineering assistance in the identification of IT vulnerabilities for client's systems. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediations. Certified Ethical Hacker (CEH) is preferred but not required.*

Cyber Security Specialist

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience

Functional Responsibility: 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, phishing, 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. Collects intrusion artifacts and responds to incidents, investigates violations, correlates data and recommends enhancements to plug potential security gaps. Performs risk analyses which also includes risk assessment, identifies, investigates, analyzes,



and remediates information security events to ensure enterprise integrity against technical and physical risks. Conducts quality management reviews to evaluate the effectiveness of security controls. This position reports on the controls effectiveness for mitigating exposure to identified risks. Communicates security issues and control gaps through security governance processes. This position implements and integrates risk management procedures across the enterprise. Participates in the development and maintenance of business continuity planning, data, systems, and network security for systems & controls related to their job duties. Provides technical support for secure software development and integration tasks, including reviewing work products for correctness and adhering to the design concept and to user standards. Knowledgeable of Security/Information Assurance (IA) products such as PKI, VPN, firewalls, and intrusion detection systems. Analyzes and recommends resolution of security/IA problems on the basis of knowledge of the major IA products and services, an understanding of their limitations, and knowledge of the IA disciplines. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation. Certified Ethical Hacker (CEH) is preferred but not required.*

Cyber Subject Matter Expert (SME) III

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 15 years of experience



Functional Responsibility: Performs as a consultant in a highly specialized, leading edge information technologies and methodologies related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides highly technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME III understands, articulates and implements best practices related to their area of expertise. The SME may lead a work-group with the need for specialized knowledge. The SME III provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business and technical solutions. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation. Certified Ethical Hacker (CEH) is preferred but not required.*

Cyber Subject Matter Expert (SME) II

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 5 years of experience



Functional Responsibility: Under general guidance, performs as a consultant in a highly specialized, leading edge information technologies and methodologies related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides highly technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME II understands, articulates and implements best practices related to their area of expertise. The SME II provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their advanced skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement business and technical solutions. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation. Certified Ethical Hacker (CEH) is preferred but not required.*

Cyber Subject Matter Expert (SME) I

Minimum Education: Bachelor's Degree or equivalent substitution

Minimum/General Experience: 2 years of experience

Functional Responsibility: Under specific direction, performs as a consultant in highly specialized, leading edge information technologies and methodologies



related to IT areas including, but not limited to Systems, Facilities, Programming, Security Services, Data Conversion, Security and Networking. Provides technical and specialized guidance concerning automated solutions to complex information processing problems. Performs elaborate analysis and studies. Prepares reports and gives presentations. The SME I understands, articulates and implements best practices related to their area of expertise. Working with a team, the SME I provides guidance on how their area of capability can resolve an organizational need and actively participates projects involving the Network, Security or Enterprise architecture or in phases of the Software and Hardware development life cycle. Apply their skills and experience in systems development, detailed knowledge of business processes, technical background and supervisory skills to implement solutions. *Specialized tasks may include but are not limited to ethical hacking, penetration testing or risk and vulnerability assessment (RVA), whether related to potential or actual threats, attacks, incidents, forensics, intrusions, and/or responses/remediation. Certified Ethical Hacker (CEH) is preferred but not required.*