BRTRC Federal Solutions, Inc.
11790 Sunrise Valley Dr
Reston, VA 20191
Voice: 703-414-5015 Email: dana.ho@wbbinc.com
Website: https://www.wbbinc.com
Business Size: Large Business

Contract Number: GS35F537AA
Period Covered by Contract: Sep 9, 2018-Sep 8, 2023
Pricelist current through Modification Number PS-A812, effective May 15, 2020.

Products and ordering information in this Authorized Information Technology Schedule Pricelist are also available on the GSA Advantage! System (http://www.gsaadvantage.gov).
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information for Ordering Activities Applicable to All Special Item Numbers</td>
<td>3</td>
</tr>
<tr>
<td>Terms and Conditions to SINs 54151S and 54151HACS</td>
<td>5 and 19</td>
</tr>
<tr>
<td>Labor Category Descriptions and Pricing</td>
<td>8, 23, 27, 31 and 35</td>
</tr>
</tbody>
</table>

*Products and ordering information in this Authorized Information Technology Schedule Pricelist are also available on the GSA Advantage! System (http://www.gsaadvantage.gov).*
INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s). See page 8, 23, 27, 31 and 35

2. Maximum order - $500,000.00 for SIN 54151HACS

3. Minimum order - $100.00

4. Geographic coverage (delivery area) - The Geographic Scope of Contract will be domestic and overseas delivery

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

   11790 Sunrise Valley Dr, Reston, VA 20191

6. Discount from list prices or statement of net price – See page 8, 23, 27, 31 and 35

7. Quantity discounts - N/A

8. Prompt payment terms – Net 30 Days

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

10a. Time of delivery - As determined by the Task Order

10b. Expedited Delivery. The Contractor will insert the sentence “Items available for expedited delivery are noted in this price list.” under this heading. The Contractor may use a symbol of its choosing to highlight items in its price lists that have expedited delivery – Need to contact BRTRC

10c. Overnight and 2-day delivery. The Contractor will indicate whether overnight and 2-day delivery are available. Also, the Contractor will indicate that the schedule customer may contact the Contractor for rates for overnight and 2-day delivery - Need to contact BRTRC

10d. 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 - Need to contact BRTRC

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

12a. Ordering address(es).

   11790 Sunrise Valley Dr, Reston, VA 20191

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

13. Payment address(es).

   11790 Sunrise Valley Dr, Reston, VA 20191

14. Warranty provision. Standard
15. Export packing charges, if applicable. N/A

16. Terms and conditions of Government purchase card acceptance (any thresholds above the micro-purchase level).

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

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

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

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

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

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

22. Preventive maintenance (if applicable). N/A

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants). N/A

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

25. Data Universal Number System (DUNS) number. 161244280

26. Notification regarding registration in the System for Award Management (SAM) database. Registered

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/IAM 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 1-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/IAM 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/IAM Professional Services.

9. **INDEPENDENT CONTRACTOR**

All IT/IAM 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/IAM 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/IAM PROFESSIONAL SERVICES AND PRICING**

Refer to the Labor Category Rates in the following table and the Labor Category Descriptions on the next page for a description of services and pricing offered for SIN **54151S**

<table>
<thead>
<tr>
<th>Labor Categories</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager Senior</td>
<td>$181.90</td>
</tr>
<tr>
<td>Project Manager</td>
<td>$139.94</td>
</tr>
<tr>
<td>Subject Matter Expert - Lead</td>
<td>$199.50</td>
</tr>
<tr>
<td>Subject Matter Expert - Senior</td>
<td>$174.56</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$164.58</td>
</tr>
<tr>
<td>Security Architect - Principal</td>
<td>$182.04</td>
</tr>
<tr>
<td>Security Architect – Lead</td>
<td>$166.79</td>
</tr>
<tr>
<td>Security Architect - Senior</td>
<td>$148.44</td>
</tr>
<tr>
<td>Security Architect</td>
<td>$139.55</td>
</tr>
<tr>
<td>Systems Engineer - Principal</td>
<td>$168.91</td>
</tr>
<tr>
<td>Systems Engineer - Lead</td>
<td>$145.76</td>
</tr>
<tr>
<td>Systems Engineer - Senior</td>
<td>$129.16</td>
</tr>
<tr>
<td>Systems Engineer</td>
<td>$113.94</td>
</tr>
<tr>
<td>Network Engineer - Principal</td>
<td>$160.45</td>
</tr>
<tr>
<td>Network Engineer - Lead</td>
<td>$129.15</td>
</tr>
<tr>
<td>Network Engineer - Senior</td>
<td>$124.69</td>
</tr>
<tr>
<td>Network Engineer</td>
<td>$89.77</td>
</tr>
<tr>
<td>Security Engineer - Principal</td>
<td>$166.79</td>
</tr>
<tr>
<td>Security Engineer - Lead</td>
<td>$146.70</td>
</tr>
<tr>
<td>Security Engineer - Senior</td>
<td>$129.16</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>$119.55</td>
</tr>
<tr>
<td>Security Analyst - Principal</td>
<td>$133.32</td>
</tr>
<tr>
<td>Security Analyst - Lead</td>
<td>$109.81</td>
</tr>
<tr>
<td>Security Analyst - Senior</td>
<td>$86.90</td>
</tr>
<tr>
<td>Security Analyst</td>
<td>$67.44</td>
</tr>
</tbody>
</table>
1. **Project Manager – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 12 years’ experience, of which at least 9 years must be specialized IT-related experience in managing complex IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.

Functional Responsibility: Responsible for and leads teams on large, complex IT-related projects. Translates customer IT requirements into formal agreements and plans to culminate in customer acceptance or results. Possesses expert knowledge of business processes. Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for their IT project, according to their project charter. Works with customer to identify business requirements and develops the proposal. Leads a team in the initiating, planning, controlling, executing, and closing IT tasks of a project (or segment of a project) to produce the IT solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery. Anticipates future customer, industry, and business trends related to IT. Applies this understanding to complex computer system problems to meet project objectives. Analyzes new and complex IT project-related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

2. **Project Manager**

Minimum/General Experience and Years of Experience: This position requires a minimum of 8 years’ experience, of which at least 5 years must be specialized IT-related experience in managing complex IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.

Functional Responsibility: Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for IT-related projects. Works with customer to identify business requirements and develops the proposal supporting IT-related projects. Leads a team of IT specialists in the initiating, planning, controlling, executing, and closing IT tasks of a project (or segment of a project) to produce the solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery of an IT solution. Anticipates future customer, industry, and business trends. Assesses information and situations and implements IT actions independently and through the management team, to ensure IT project objectives are met. Analyzes new and complex IT project related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.

3. **Subject Matter Expert – Lead**

Minimum/General Experience and Years of Experience: This position requires 9 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies principals and methods of the subject matter to specialized solutions. Solutions developed include but is not limited to: cyber security, information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions. May lead teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.
4. **Subject Matter Expert – Senior**

Minimum/General Experience and Years of Experience: This position requires 7 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies principals and methods of the subject matter to specialized solutions. Solutions developed include but is not limited to: cyber security, information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

5. **Subject Matter Expert**

Minimum/General Experience and Years of Experience: This position requires 5 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Supports resolution of problems which require an intimate knowledge of the related technical subject matter. Applies principals and methods of the subject matter to specialized solutions. Solutions supported include but is not limited to: cyber security, information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

6. **Security Architect – Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 11 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex INFOSEC - related technical problems. Reviews and recommends INFOSEC solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of INFOSEC products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and network security. Insures that INFOSEC solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.
Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

7. **Security Architect – Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 6 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex INFOSEC-related technical problems. Reviews and recommends INFOSEC solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of INFOSEC products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and network security. Insures that INFOSEC solutions are fully compatible with or engineered into the customer’s network design. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

8. **Security Architect – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 7 years’ experience, of which at least 4 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Develops and recommends technical solutions to support client requirements in solving moderately complex network, platform and system security problems. Typical focus areas include analytical and engineering solutions based on federal and industry INFOSEC policy, doctrine and regulations. Responsibilities include: developing solutions or providing support related to identity management, secure system engineering and development, biometrics, system/security requirements analysis, secure system definition, as well as, specification development of INFOSEC policies and procedures utilizing technical and analytical skills. Also designs test beds for the Developmental Test & Evaluation (DT&E) of advanced INFOSEC hardware and software solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

9. **Security Architect**

Minimum/General Experience and Years of Experience: This position requires a minimum of 5 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level
applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Develops and recommends technical solutions to support client’s requirements in solving network, platform and system security problems. Typical focus areas include analytical and engineering solutions based on federal and industry INFOSEC policy, doctrine and regulations. Responsibilities include supporting secure system engineering and development, including system/security requirements analysis and secure system definition and specification development of INFOSEC policies and procedures utilizing technical and analytical skills. Also helps design test beds for the DT&E of advanced INFOSEC hardware and software solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

10. Systems Engineer – Principal

Minimum/General Experience and Years of Experience: This position requires a minimum of 11 years’ experience, of which at least 8 years must be specialized experience in identifying, analyzing and resolving complex system engineering problems. Experienced in the design, installation and acceptance testing of complex systems. Applies the principles of assessing and analyzing system transmission data to resolve reported malfunctions.

Functional Responsibility: Oversees technical design, development, and implementation of large and/or complex systems. Defines architecture requirements and establishes standards for design and development. Consults with management and customers regarding product feasibility and viability of product plans and designs. Factors emerging technologies and product supportability into design and implementation. Interacts with customers regarding strategies, requirements, problem solving, and support. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

11. Systems Engineer – Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 6 years must be specialized experience in identifying, analyzing and resolving complex system engineering problems. Experienced in the design, installation and acceptance testing of complex systems. Applies the principles of assessing and analyzing system transmission data to resolve reported malfunctions.

Functional Responsibility: Designs complex business and management information systems and applications. Researches and integrates design strategies, product specifications, development schedules, and user expectations. Prepares feasibility studies of potential systems, including application architectures, computing platforms, and network configurations. Prepares detailed hardware, software, and/or network specifications. Builds, tests, and maintains product modules, components, and subsystems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.
12. **Systems Engineer – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 7 years’ experience, of which at least 4 years must be specialized experience in identifying, analyzing and resolving complex system engineering problems. Experienced in the design, installation and acceptance testing of complex systems. Applies the principles of assessing and analyzing system transmission data to resolve reported malfunctions.

Functional Responsibility: Performs engineering work in the research, development, and design of products and systems. Organizes, directs, and conducts technical efforts in systems design, engineering, and integration. Prepares technical project plans and schedules. Conducts system tests, and analyzes and quantifies test data. Prepares design documents and technical reports.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

13. **Systems Engineer**

Minimum/General Experience and Years of Experience: This position requires a minimum of 5 years’ experience, of which at least 2 years must be specialized experience in identifying, analyzing and resolving complex system engineering problems. Experienced in the design, installation and acceptance testing of complex systems. Applies the principles of assessing and analyzing system transmission data to resolve reported malfunctions.

Functional Responsibility: Performs a full range of engineering tasks including systems design, engineering, integration, configuration management, and testing. Analyzes information and data processing requirements to determine electronic or data processing system capabilities required for projects or workload. Reports on findings and provides recommendations and alternative approaches.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

14. **Network Engineer – Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 11 years’ experience, of which at least 8 years must be specialized experience in identifying, analyzing and resolving complex network hardware, software, circuit, and transmission problems. Experienced in the design, installation and acceptance testing of complex high-speed networks. Applies the principles of assessing and analyzing network transmission data to resolve reported malfunctions.

Functional Responsibility: Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social
sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

15. **Network Engineer – Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 6 years must be specialized experience in identifying, analyzing and resolving complex network hardware, software, circuit, and transmission problems. Experienced in the design, installation and acceptance testing of complex high-speed networks. Applies the principles of assessing and analyzing network transmission data to resolve reported malfunctions.

Functional Responsibility: Supports the designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex network and security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

16. **Network Engineer – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 7 years’ experience, of which at least 4 years must be specialized experience in identifying, analyzing and resolving complex network hardware, software, circuit, and transmission problems. Experienced in the design, installation and acceptance testing of complex high-speed networks. Applies the principles of assessing and analyzing network transmission data to resolve reported malfunctions.

Functional Responsibility: Supports the designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

17. **Network Engineer**

Minimum/General Experience and Years of Experience: This position requires a minimum of 5 years’ experience, of which at least 2 years must be specialized experience in identifying, analyzing and resolving complex network hardware, software, circuit, and transmission problems. Experienced in the design, installation and acceptance testing of complex high-speed networks. Applies the principles of assessing and analyzing network transmission data to resolve reported malfunctions.

Functional Responsibility: Under some supervision helps design and coordinate the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options.
Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

18. **Security Engineer – Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 11 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to computer security requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel. Anticipates future customer, industry, and business trends. Information and situations and implements actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

19. **Security Engineer – Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 6 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to computer security requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the
work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

20. **Security Engineer – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 7 years experience, of which at least 4 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Develops, engineers, and implements solutions to computer security requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Helps design and coordinate the installation and acceptance testing of networks and network components. Isolates, resolves, or circumvents network problems. Monitors network hardware operations to ensure properly set configuration options. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

21. **Security Engineer**

Minimum/General Experience and Years of Experience: This position requires a minimum of 5 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Supports the development, engineering, and implementation of solutions to computer security requirements. Supports the collecting and organizing of technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

22. **Security Analyst – Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 6 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to computer security requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational
capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

23. Security Analyst – Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 7 years’ experience, of which at least 4 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to computer security requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing analysis activities related to security tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

24. Security Analyst – Senior

Minimum/General Experience and Years of Experience: This position requires a minimum of 5 years’ experience, of which at least 3 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and helps analyze and define security requirements. Helps develop, engineer, and implement solutions to computer security requirements. Collects, organizes technical information about an organization’s computer security requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs security risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

25. Security Analyst

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 1 year must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.
Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Helps develop, engineer, and implement solutions to computer security requirements. Collects and organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Develops documentation supporting activities performed. Provides support in an operational capacity to security-related activities. Helps perform risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
(SPECIAL ITEM NUMBERS 54151HACS)

****NOTE: Non-professional labor categories must be incidental to, and used solely to support Highly Adaptive Cybersecurity Services, and cannot be purchased separately. Further, non-professional labor categories shall be offered under SIN 54151HACS only.

****NOTE: Labor categories under the Special Item Number 132-51 Information Technology Professional Services may remain under SIN 132-51 unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.

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 800-44 - 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 Numbers 54151HACS High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.
   b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70, and may be quoted along with services to provide a total solution.
   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

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” 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. 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.

12. 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.

13. 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.

14. 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.

15. RESUMES

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

**LABOR CATEGORY DESCRIPTIONS AND PRICING FOR SINS 54151HACS**

<table>
<thead>
<tr>
<th>Labor Categories</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager Senior</td>
<td>$164.23</td>
</tr>
<tr>
<td>Subject Matter Expert - Lead</td>
<td>$197.51</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$167.88</td>
</tr>
<tr>
<td>Security Architect - Principal</td>
<td>$185.37</td>
</tr>
<tr>
<td>Security Engineer - Principal</td>
<td>$165.12</td>
</tr>
<tr>
<td>Security Engineer - Lead</td>
<td>$148.17</td>
</tr>
<tr>
<td>Security Engineer - Senior</td>
<td>$127.50</td>
</tr>
<tr>
<td>Security Analyst - Lead</td>
<td>$118.47</td>
</tr>
</tbody>
</table>
1. **Project Manager - Senior**

   Minimum/General Experience and Years of Experience: This position requires a minimum of 10 years’ experience in managing complex Cybersecurity and IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.

   Functional Responsibility: Responsible for and leads teams on large, complex Cybersecurity-related projects. Translates customer requirements into formal agreements and plans to culminate in customer acceptance or results. Possesses expert knowledge of business processes. Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for their Penetration Testing project, according to their project charter. Works with customer to identify business requirements and develops the proposal. Leads a team in the initiating, planning, controlling, executing, and closing Cybersecurity tasks of a project (or segment of a project) to produce the Cybersecurity solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery. Anticipates future customer, industry, and business trends related to Cybersecurity. Applies this understanding to complex computer system problems to meet project objectives. Analyzes new and complex Cybersecurity project-related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.

   Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

2. **Subject Matter Expert - Lead**

   Minimum/General Experience and Years of Experience: This position requires 10 years of intensive and progressive experience in the applicable specialty field.

   Functional Responsibility: Applies subject matter knowledge in Cybersecurity and Penetration Testing to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions developed may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions. May lead teams or small groups of personnel in performing complex security-related tasks.

   Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

3. **Subject Matter Expert**

   Minimum/General Experience and Years of Experience: This position requires 7 years of intensive and progressive experience in the applicable specialty field.
Functional Responsibility: Applies Cybersecurity and Penetration Testing subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Supports resolution of problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions supported may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

4. **Security Architect - Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex Cybersecurity - related technical problems. Reviews and recommends Penetration Testing solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of Cybersecurity products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and Cybersecurity. Insures that Cybersecurity solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

5. **Security Engineer - Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 4 years’ experience, of which at least 3 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines Cybersecurity requirements. Develops, engineers, and implements solutions to Penetration Testing requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under
deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options with Cybersecurity focus. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel. Anticipates future customer, industry, and business trends. Information and situations and implements actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

6. Security Engineer - Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to Cybersecurity problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Penetration Testing requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

7. Security Engineer – Senior

Minimum/General Experience and Years of Experience: This position requires a minimum of 2 years’ experience, of which at least 1 year must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Develops, engineers, and implements solutions to Penetration Testing requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Helps design and coordinate the installation and acceptance testing of networks and network components.
Isolates, resolves, or circumvents network problems. Monitors network hardware operations to ensure properly set configuration options. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

8. Security Analyst - Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Penetration Testing requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting Cybersecurity activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing analysis activities related to security tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

LABOR CATEGORY DESCRIPTIONS AND PRICING FOR SIN 54151HACS - Site Only

<table>
<thead>
<tr>
<th>Labor Categories</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager Senior</td>
<td>$164.23</td>
</tr>
<tr>
<td>Subject Matter Expert - Lead</td>
<td>$197.51</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$167.88</td>
</tr>
<tr>
<td>Security Architect - Principal</td>
<td>$185.37</td>
</tr>
<tr>
<td>Security Engineer - Principal</td>
<td>$165.12</td>
</tr>
<tr>
<td>Security Engineer - Lead</td>
<td>$148.17</td>
</tr>
<tr>
<td>Security Engineer - Senior</td>
<td>$127.50</td>
</tr>
<tr>
<td>Security Analyst - Lead</td>
<td>$118.47</td>
</tr>
</tbody>
</table>

1. Project Manager - Senior

Minimum/General Experience and Years of Experience: This position requires a minimum of 10 years’ experience in managing complex Cybersecurity and IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.
Functional Responsibility: Responsible for and leads teams on large, complex Cybersecurity-related projects. Translates customer requirements into formal agreements and plans to culminate in customer acceptance or results. Possesses expert knowledge of business processes. Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for their Incident Response project, according to their project charter. Works with customer to identify business requirements and develops the proposal. Leads a team in the initiating, planning, controlling, executing, and closing Cybersecurity tasks of a project (or segment of a project) to produce the Cybersecurity solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery. Anticipates future customer, industry, and business trends related to Cybersecurity. Applies this understanding to complex computer system problems to meet project objectives. Analyzes new and complex Cybersecurity project-related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

2. Subject Matter Expert - Lead

Minimum/General Experience and Years of Experience: This position requires 10 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge in Cybersecurity and Incident Response to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions developed may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions. May lead teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

3. Subject Matter Expert

Minimum/General Experience and Years of Experience: This position requires 7 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies Cybersecurity and Incident Response subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Supports resolution of problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions supported may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.
Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

4. **Security Architect - Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex Cybersecurity-related technical problems. Reviews and recommends Incident Response solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of Cybersecurity products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and Cybersecurity. Insures that Cybersecurity solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

5. **Security Engineer - Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 4 years’ experience, of which at least 3 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines Cybersecurity requirements. Develops, engineers, and implements solutions to Incident Response requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options with Cybersecurity focus. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel. Anticipates future customer, industry, and business trends. information and situations and implements actions independently and or through the management team.
Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

6. **Security Engineer - Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to Cybersecurity problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Incident Response requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

7. **Security Engineer – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 2 years’ experience, of which at least 1 year must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Develops, engineers, and implements solutions to Incident Response requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Helps design and coordinate the installation and acceptance testing of networks and network components. Isolates, resolves, or circumvents network problems. Monitors network hardware operations to ensure properly set configuration options. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.
8. **Security Analyst - Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Incident Response requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting Cybersecurity activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing analysis activities related to security tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

**LABOR CATEGORY DESCRIPTIONS AND PRICING FOR 54151HACS, Cyber Hunt - Site Only**

<table>
<thead>
<tr>
<th>Labor Categories</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager Senior</td>
<td>$164.23</td>
</tr>
<tr>
<td>Subject Matter Expert - Lead</td>
<td>$197.51</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$167.88</td>
</tr>
<tr>
<td>Security Architect - Principal</td>
<td>$185.37</td>
</tr>
<tr>
<td>Security Engineer - Principal</td>
<td>$165.12</td>
</tr>
<tr>
<td>Security Engineer - Lead</td>
<td>$148.17</td>
</tr>
<tr>
<td>Security Engineer - Senior</td>
<td>$127.50</td>
</tr>
<tr>
<td>Security Analyst - Lead</td>
<td>$118.47</td>
</tr>
</tbody>
</table>

1. **Project Manager - Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 10 years’ experience in managing complex Cybersecurity and IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.

Functional Responsibility: Responsible for and leads teams on large, complex Cybersecurity -related projects. Translates customer requirements into formal agreements and plans to culminate in customer acceptance or results. Possesses expert knowledge of business processes. Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for their Cyber Hunt project, according to their project charter. Works with customer to identify business requirements and develops the proposal. Leads a team in the initiating, planning, controlling, executing, and closing Cybersecurity tasks of a project (or segment of a project) to produce the
Cybersecurity solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery. Anticipates future customer, industry, and business trends related to Cybersecurity. Applies this understanding to complex computer system problems to meet project objectives. Analyzes new and complex Cybersecurity project-related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

2. **Subject Matter Expert - Lead**

Minimum/General Experience and Years of Experience: This position requires 10 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge in Cybersecurity and Cyber Hunt to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions developed may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions. May lead teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

3. **Subject Matter Expert**

Minimum/General Experience and Years of Experience: This position requires 7 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies Cybersecurity and Cyber Hunt subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Supports resolution of problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions supported may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

4. **Security Architect - Principal**
Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex Cybersecurity-related technical problems. Reviews and recommends Cyber Hunt solutions to customer problems based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of Cybersecurity products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and Cybersecurity. Insures that Cybersecurity solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

5. Security Engineer - Principal

Minimum/General Experience and Years of Experience: This position requires a minimum of 4 years’ experience, of which at least 3 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines Cybersecurity requirements. Develops, engineers, and implements solutions to Cyber Hunt requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options with Cybersecurity focus. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel. Anticipates future customer, industry, and business trends, information and situations and implements actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

6. Security Engineer - Lead
Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to Cybersecurity problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Cyber Hunt requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

7. Security Engineer – Senior

Minimum/General Experience and Years of Experience: This position requires a minimum of 2 years’ experience, of which at least 1 year must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Develops, engineers, and implements solutions to Penetration Testing requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Helps design and coordinate the installation and acceptance testing of networks and network components. Isolates, resolves, or circumvents network problems. Monitors network hardware operations to ensure properly set configuration options. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

8. Security Analyst - Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.
Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Cyber Hunt requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting Cybersecurity activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing analysis activities related to security tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

LABOR CATEGORY DESCRIPTIONS AND PRICING FOR SIN 54151HACS
Site Only

<table>
<thead>
<tr>
<th>Labor Categories</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager Senior</td>
<td>$164.23</td>
</tr>
<tr>
<td>Subject Matter Expert - Lead</td>
<td>$197.51</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$167.88</td>
</tr>
<tr>
<td>Security Architect - Principal</td>
<td>$185.37</td>
</tr>
<tr>
<td>Security Engineer - Principal</td>
<td>$165.12</td>
</tr>
<tr>
<td>Security Engineer - Lead</td>
<td>$148.17</td>
</tr>
<tr>
<td>Security Engineer - Senior</td>
<td>$127.50</td>
</tr>
<tr>
<td>Security Analyst - Lead</td>
<td>$118.47</td>
</tr>
</tbody>
</table>

1. Project Manager - Senior

Minimum/General Experience and Years of Experience: This position requires a minimum of 10 years’ experience in managing complex Cybersecurity and IT projects supporting all aspects of project management including performance, cost, scope, schedule, and quality.

Functional Responsibility: Responsible for and leads teams on large, complex Cybersecurity-related projects. Translates customer requirements into formal agreements and plans to culminate in customer acceptance or results. Possesses expert knowledge of business processes. Responsible for performance, cost, scope, schedule, quality, and appropriate business measurements for their Risk and Vulnerability Assessment project, according to their project charter. Works with customer to identify business requirements and develops the proposal. Leads a team in the initiating, planning, controlling, executing, and closing Cybersecurity tasks of a project (or segment of a project) to produce the Cybersecurity solution deliverable. Executes a wide range of process activities beginning with the request for proposal through development, test, and final delivery. Anticipates future customer, industry, and business trends related to Cybersecurity. Applies this understanding to complex computer system problems to meet project objectives. Analyzes new and complex Cybersecurity project-related problems and creates innovative solutions involving finance, scheduling, computer system technology, methodology, tools and solution components.
Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

2. **Subject Matter Expert - Lead**

Minimum/General Experience and Years of Experience: This position requires 10 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies subject matter knowledge in Cybersecurity and Risk and Vulnerability Assessment to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Resolves problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions developed may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions. May lead teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

3. **Subject Matter Expert**

Minimum/General Experience and Years of Experience: This position requires 7 years of intensive and progressive experience in the applicable specialty field.

Functional Responsibility: Applies Cybersecurity and Risk and Vulnerability Assessment subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration, installation, documentation, and implementation. Supports resolution of problems which require an intimate knowledge of the related technical subject matter. Applies Cybersecurity principals and methods of the subject matter to specialized solutions. Solutions supported may include adjacent or related areas to Cybersecurity including: information assurance, network engineering, application assessment and development, solution deployment and integration, system engineering, information technology solutions.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

4. **Security Architect - Principal**

Minimum/General Experience and Years of Experience: This position requires a minimum of 9 years’ experience, of which at least 8 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Provides customer support in solving all phases of complex Cybersecurity-related technical problems. Reviews and recommends Risk and Vulnerability Assessment solutions to customer problems.
based on an understanding of products/systems test results. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration and testing of Cybersecurity products and techniques. Solutions are based on a firm understanding of government/industry policy, practices, procedures, and customer requirements. Particular attention placed on Guard, Firewall, Secure Network Server, “Smart Cards”, and emerging security technologies and future trends in support of information system and Cybersecurity. Insures that Cybersecurity solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

5. Security Engineer - Principal

Minimum/General Experience and Years of Experience: This position requires a minimum of 4 years’ experience, of which at least 3 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines Cybersecurity requirements. Develops, engineers, and implements solutions to Risk and Vulnerability Assessment requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options with Cybersecurity focus. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel. Anticipates future customer, industry, and business trends. information and situations and implements actions independently and or through the management team.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

6. Security Engineer - Lead

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to Cybersecurity problems.
Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Risk and Vulnerability Assessment requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Designs and coordinates the installation and acceptance testing of the system network. Monitors network hardware operations to ensure properly set configuration options. Plans implementation of enhancements and upgrades to the network; performs cost/benefit studies of network configurations and recommends enhancements; directs acquisition, installation, and testing of network hardware; advises network users of hardware requirements, configurations, and limitations; and isolates, resolves, or circumvents network problems. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

7. **Security Engineer – Senior**

Minimum/General Experience and Years of Experience: This position requires a minimum of 2 years’ experience, of which at least 1 year must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Typically supports more senior personnel and analyzes and defines security requirements. Develops, engineers, and implements solutions to Risk and Vulnerability Assessment requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Helps design and coordinate the installation and acceptance testing of networks and network components. Isolates, resolves, or circumvents network problems. Monitors network hardware operations to ensure properly set configuration options. Performs in an operational capacity supporting security-related activities. Performs risk analyses which may include risk assessments.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.

8. **Security Analyst - Lead**

Minimum/General Experience and Years of Experience: This position requires a minimum of 3 years’ experience, of which at least 2 years must be specialized experience in defining security requirements for high level applications, evaluation of approved security product capabilities, and developing solutions to computer security problems.

Functional Responsibility: Analyzes and defines security requirements. Develops, engineers, and implements solutions to Risk and Vulnerability Assessment requirements. Collects, organizes technical information about an organization’s requirements and objectives, existing security products, and ongoing security posture. Performs in an operational capacity supporting Cybersecurity activities. Performs risk analyses which may include risk assessments. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel.
personnel, operates under deadlines, able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing analysis activities related to security tasks.

Educational Requirements: A Bachelor’s degree in computer science/systems, information systems/technology, engineering/engineering technology, software engineering/programming, management, natural sciences, social sciences, mathematics, or business/finance. Education and experience requirements may be substituted with comparable years’ experience or with advanced degrees or advanced certifications.