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

**Multiple Award Schedule (MAS)**

**Contract Number:** GS-35F-0232X

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

**Contract Period:** February 15, 2021, to February 14, 2026

Price list current through Mod No. PO-0038 dated January 15, 2021

**Network Security Systems Plus, Inc.**

1751 Pinnacle Dr., Suite 600  
McLean, VA  22102-4007

**Phone:** 703-933-7040  
**Website:** www.nssplus.com  
**Business Size:** Small Disadvantaged Veteran-Owned  
**Contract Administrator:** Wayne S. Clark  
**Phone:** 703-835-9773  
**Email:** Wayne.Clark@NSSPlus.com

Prices Shown Herein are Net (discount deducted).
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUSTOMER INFORMATION</td>
<td>1</td>
</tr>
<tr>
<td>TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)</td>
<td>2</td>
</tr>
<tr>
<td>USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS</td>
<td>6</td>
</tr>
<tr>
<td>BEST VALUE BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE</td>
<td>7</td>
</tr>
<tr>
<td>BPA FORMAT GUIDELINES</td>
<td>8</td>
</tr>
<tr>
<td>BASIC GUIDELINES FOR USING “CONTRACTOR TEAM ARRANGEMENTS”</td>
<td>10</td>
</tr>
<tr>
<td>CONTRACTOR’S INFORMATION TECHNOLOGY LABOR CATEGORY DESCRIPTIONS</td>
<td>11</td>
</tr>
<tr>
<td>54151S GSA Labor Category Descriptions</td>
<td>11</td>
</tr>
<tr>
<td>54151HACS GSA Labor Category Descriptions</td>
<td>14</td>
</tr>
<tr>
<td>54151HEAL GSA Labor Category Descriptions</td>
<td>26</td>
</tr>
<tr>
<td>CONTRACTOR’S AWARDED GSA PRICING</td>
<td>30</td>
</tr>
<tr>
<td>54151S – Awarded GSA Hourly Rates</td>
<td>30</td>
</tr>
<tr>
<td>54151HACS – Awarded GSA Hourly Rates</td>
<td>31</td>
</tr>
<tr>
<td>54151HEAL – Awarded GSA Hourly Rates</td>
<td>33</td>
</tr>
</tbody>
</table>
CUSTOMER INFORMATION

1a. Table of Awarded Special Item Number(s):

<table>
<thead>
<tr>
<th>SIN</th>
<th>SIN Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Information Technology Professional Services</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Highly Adaptive Cybersecurity Services (HACS)</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health Information Technology Services</td>
</tr>
<tr>
<td>OLM</td>
<td>Order-Level Materials (OLM)</td>
</tr>
</tbody>
</table>

1b. Labor Category rates proposed in support of all SINS and is valid for all sites.

1c. Hourly Rates (Services only): See individual section by SIN for Labor Category Descriptions.

2. Maximum Order Threshold: $500,000

3. Minimum Order Threshold: $100.00

4. Geographic Coverage: Domestic delivery (48 contiguous states, and Washington, DC) for SINs 54151HACS and 54151S. Worldwide for SIN 54151HEAL.

5. Points of Productions: McLean, VA

6. Discount from List Prices or Statement of Net Price: Please see pricing matrixes (below). Negotiated discounts are applied.

7. Quality Discounts: None

8. Prompt Payment Terms: Net 30 days

9. Foreign Items: None


10b. Expedited Delivery: To be negotiated between NSSPlus, Inc., and the ordering agency.

10c. Overnight and 2-Day Delivery: Contact the contractor for

10d. Urgent Requirements: In regards to the “Urgent Requirements” clause, agencies are advised to contact the contractor for Urgent delivery requirements.

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

1751 Pinnacle Dr., Suite 600  
McLean, VA 22102-4007  
POC: Wayne S. Clark  
Phone: 703-835-9773  
Fax: 703-997-1476  
www.nssplus.com

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):** Network Security Systems Plus, Inc.  
P.O. Box 3351  
Merrifield, VA 22116-3351

14. **Warranty Provision:** Contractor's Best Effort for all Professional Services.

15. **Export Packing Charges:** N/A

16. **Terms and Conditions of Rental, Maintenance, and Repair (if applicable):** N/A

17. **Terms and Conditions of Installation (if applicable):** N/A

18a. **Terms and Conditions of Repair Parts Indicating Date of Parts Price Lists and Any Discounts from List Prices (if applicable):** N/A

18b. **Terms and Conditions for Any Other Services (if applicable):** N/A

19. **List of Service and Distribution Points (if applicable):** N/A

20. **List of Participating Dealers (if applicable):** N/A

21. **Preventative Maintenance (if applicable):** N/A

22a. **Environmental Attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants):** N/A

22b. **If applicable, indicate that Section 508 compliance information is available on Electronic and Information Technology (EIT) supplies and services and show where full details can be found (e.g., contractor’s website or other location.)** The EIT standards can be found at [www.Section508.gov/](http://www.Section508.gov/). N/A

23. **Data Universal Number System (DUNS) number:** 132705141

24. **Notification regarding registration in System for Award Management (SAM) database:** Registered. Valid until and shall be updated annually.

25. **Information for Ordering Offices:**  
   **Type of Contractor:** Small Disadvantaged Veteran–Owned Small Business  
   **Contractor’s Taxpayer Identification Number (TIN):** 16-1651100  
   **CAGE Code:** 3GPP8  
   **DUNS No.:** 132705141
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
   b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

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

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

4. PERFORMANCE OF SERVICES
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
   b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
   c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
   d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.
5. **STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)**

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

   1. Cancel the stop-work order; or
   2. Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

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

   1. The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
   2. The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

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

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

6. **INSPECTION OF SERVICES**


7. **RESPONSIBILITIES OF THE CONTRACTOR**

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

8. **RESPONSIBILITIES OF THE ORDERING ACTIVITY**

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

9. **INDEPENDENT CONTRACTOR**

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

a. Definitions.

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

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

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

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

11. INVOICES

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

12. PAYMENTS

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

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

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

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

13. RESUMES

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

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

15. APPROVAL OF SUBCONTRACTS

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING

a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 54151S IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

**IT Systems Analysis Services**

We work with our customer base to identify short and long term business needs to map those needs to actual Information Technology requirements. Our process is methodology driven and designed to help the customer meet their Information Technology goals. Our System Analysis Services’ model is centered and targeted toward the Information Assurance market space with extensive experience in developing policies, procedures, guidelines and processes to defend, certify, and secure network enterprises from external and internal adversaries.

**Automated Information Systems Design & Integration Services**

Our automated Information Systems Design & Integration Services are Information Assurance driven with special emphasis on integrating security services and component products to ensure and establish adequate levels of Information Assurance to our customer’s network enterprise.

Our extensive international business management experience has allowed for many years disaster recovery and business continuance from natural disasters such as hurricanes, floods, and earthquakes.

Network Security Systems Plus, Inc. has established certified business relationships with large security vendors such as Internet Security Systems, allowing a focus on security consulting services.

**IT Backup and Security Services**

Network Security Systems Plus, Inc. is an Information Assurance and Security network enterprise solution company. Our primary service expertise is based on defending and securing networks.

b. Pricing for all IT Professional Services shall be in accordance with the Contractor’s customary commercial practices, e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented:

**EXAMPLE:** Commercial Job Title: System Engineer

Minimum/General Experience: Three (3) years of technical experience which applies to systems analysis and design techniques for complex computer systems. Requires competence in all phases of systems analysis techniques, concepts and methods; also requires knowledge of available hardware, system software, input/output devices, structure and management practices.

Functional Responsibility: Guides users in formulating requirements, advises alternative approaches, conducts feasibility studies.

Minimum Education: Bachelor’s Degree in Computer Science
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact:

Network Security Systems Plus, Inc.
1751 Pinnacle Dr., Suite 600
McLean, VA  22102
Attn: Wayne Clark
E-mail: Wayne.Clark@NSSPlus.com
Tele: (703) 835-9773
BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE

(Insert Customer Name)

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

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

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

Signatures

Ordering Activity Date       Contractor Date
(CUSTOMER NAME)

BLANKET PURCHASE AGREEMENT

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

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

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

2. Delivery:

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

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

4. This BPA does not obligate any funds.

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

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

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

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

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

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

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

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

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

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

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

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

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

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customer’s needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.
54151S GSA Labor Category Descriptions

1. Commercial Job Title: Program Manager (PM)

   **Functional Responsibility:** Provide effective leadership, oversight, development and program management over programs, projects, and Task Orders. Develop and establish Standard Operating Procedures and implement policies and procedures in accordance with government directives. Work with the government Program Office to identify funding source and develop and maintain program execution budgets. Establish strategic goals and objectives and report program performance and budget actual against plan to the corporate Program Management Office (PMO). Manage innovation initiatives and maintain direct responsible for the reduction of cost and time associated with process improvements.

   Manages the technical direction of programs and projects in accordance with corporate policies and procedures and provide cost, schedule, risk, quality assurance and control of information to the Government Program Office. The PM reports to the PMO and will have overall responsibility for the Quality Assurance (QA) and Quality Control (QC) for the work, deliverables, processes, and daily operations of the program. Performs assessments and evaluations of program(s) and process components; validate results, report discrepancies; and follows through to ensure that all issues are resolved on a timely basis.

   The PM will be responsible for the effective management of all tasks associated with a program and will maintain responsible for ensuring customer satisfaction and oversees technology and resource allocation. The PM will also participate in pre-award/post award and transition planning and organizing to ensure that each task is perform efficiently, accurately, on time, and in compliance with the contract requirements. The PM will coordinate when applicable with the government Program Manager and the Contracting Officer Representative (COR) to ensure that the program is manage consistently with overall contract requirements and will ensure timely and accurate submission of invoices.

   **Certifications:** Project Management Professional (PMP).

   **Education:** Bachelor’s Degree in Information System or Business Finance Management or Computer Sciences or related discipline.

   **Experience:** Requires a minimum of 15 years of technical engineering experience and 5 or more years of program management experience in assigned business area.

2. Commercial Job Title: Subject Matter Expert 5 (SME5)

   **Functional Responsibility:** The SME5 is responsible for the management of a team of engineers, analysts and project contributors. He/She is directly responsible for the analysis and development of technical engineering documentation that is delivered to the government for approval. The SME5 is required to supervise the work of the SME4, SME3, and SME2 to ensure that the customer Standard OPERATING Procedures are being followed. The SME5 is also responsible for the creation of Configuration Management documentation. The SME5 also provides technical leadership and guidance to the SME4 and SME3 during the implementation of solutions for the customer’s network. He/She is required to verify that all devices are under the configuration management process. In addition, the SME5 is responsible for leading the weekly team meetings with the customer and providing status reports to senior management.

   To carry-out the engineering and management responsibilities identified above, The SME5 must exhibit the experience and ability to provide enterprise-wide technical management and direction for problem definition,
analysis and requirements development and implementation for very complex IT systems in the subject matter area. Additionally, this individual has the ability to provide workable recommendations and advice to client executive management on emerging technology, system improvements, optimization and maintenance in the following areas: Information Systems Architecture, Automation, Telecommunications, Networking, Communication Protocols, Software, Electronic Email, Modeling and Simulation, Data Storage and Retrieval. The SME5 must have the required experience and ability to provide technical management and direction for problem definition, analysis and requirements development and implementation for complex IT systems in the subject matter area.

Education: Bachelor’s Degree in Computer Science or related field; a Master Degree in Computer Science of Engineering is a preferred and a certification in Certified Information Systems Security Professional (CISSP) or equivalent specialized certification in technical discipline is required.

Experience: At least ten (10) years of progressive applied technical experience with complex Enterprise IT systems and Networks.

3. Commercial Job Title: Subject Matter Expert 4 (SME4)

Functional Responsibility: The SME4 reports to a Program Manager or SME5 as a member of the technical team. He/She is responsible for providing technical/engineering assistance to the project. The SME4 is required to provide technical input to the configuration management process. The SME4 must exhibit the technical ability and know-how to conduct technical analysis using automated tools and checklist to develop and implement solutions for large enterprise networks. The SME4 must have technical knowledge of database management systems and applications. He/She must have the ability to effectively communicate network vulnerabilities and required safeguards to the customer’s engineering staff. In addition, the SME4 is responsible for uploading network scan results to the automated system and to interface with the customer to communicate, interpret and analyze technical results.

This individual exhibits the ability to assist the project team in providing workable recommendations and advice on system improvements, optimization, and maintenance in the following areas: Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.

Education: Bachelor’s Degree in Computer Science or related field is required; a certification in an IT technical discipline is required.

Experience: At least seven (7) years of progressive applied technical experience with complex IT network.

4. Commercial Job Title: Subject Matter Expert 3 (SME3)

Functional Responsibility: The SME3 reports to a Program Manager or SME5 and is required to have experience in conducting technical reviews of system documentation and providing quality assurance on all of the configuration management documentation package. SME3 is also responsible for working under the technical supervision of the SME4 and SME5 to assist with the assessment of the enterprise environment. The SME3 duties entail that he or she carry-out and completes technical tasks requiring a lower level of technical expertise and is responsible for the preparation of the configuration documentation. The SME3 must have the ability to effectively communicate the customer’s requirements to the SME4 and SME5 and make recommendations and advise on organization-wide process improvements.

In summary, this individual in conjunction with directives laid out by SME4 and SME5 has the ability to coordinate and manage the preparation of analysis, evaluations, and recommendations for proper implementation
of programs and systems specifications in the following specialties: Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.

**Education:** Bachelor’s Degree in Computer Science or related field; an associate level certification is required from CompTIA or equivalent recognized organization.

**Experience:** At least three (3) years of progressive applied technical experience with IT systems.

5. **Commercial Job Title: Subject Matter Expert 2 (SME2)**

**Functional Responsibility:** Defines the problems and analyzes and develops plans and requirements in the subject matter area for simple to moderately complex systems. Consults directly with client to define need, obtains required data, and analyzes data to advise on or recommend solution. Provides technical expertise in a specific technical area, typically translating raw data into concise documentation for technical higher-level SME’s and complimentary non-technical staff. The SME2 reports directly to the SME 4 and SME5, providing overall quality assurance for the configuration management package. Duties also entail that this individual provides technical review, technical writing, and generates summaries, reports and presentations, such as technology assessments and program audits. Individual has demonstrated competence using data from project management tools - simultaneously planning and managing with higher level SME team the transition of highly technical projects from planning to execution of tasks.

In summary, this individual has ability, in conjunction with our team of subject matter experts, to coordinate and manage the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in the following specialties: Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.

**Education:** Bachelor’s degree in Computer Science, Business, or related field is required; an associate level certification is required from CompTIA or equivalent recognized organization.

**Experience:** At least two (2) years of progressive applied technical experience with simple to moderately complex IT systems.

6. **Commercial Job Title: Help Desk Specialist (Senior Level)**

**Functional Responsibility:** Under general supervision provides tier 2 support to end users for PC, service, mainframe applications, and hardware. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends system modifications to reduce user problems. Maintains currency and highest-level technical skills in field of expertise. Demonstrated ability to assist in the use of software and hardware, servers, printers, network components, and other peripheral components. Ability to conduct component level diagnostics. Demonstrated ability to assist in the use of a variety of business software and operating systems. Ability to develop and maintain documentation for procedures and processes, as well as maintenance logs and equipment databases. Ability to effectively communicate orally and in writing. Ability to teach hardware concepts to customers with little or no background in computers.

**Education:** Associate degree or equivalent experience with CompTIA certification.

**Experience:** Six (6) Months of applied experience.
54151HACS GSA Labor Category Descriptions

1. Commercial Job Title: Penetration Tester 1

Functional Responsibility: The Penetration Tester 1 contributes to the external assessment process by conducting passive and active reconnaissance, social engineering, and internal and external attack plans under the direction of the penetration testing lead.

Conduct open source research on target sites and personnel to include use of pre-texting; Participate in developing after action reports, out briefs and vulnerability mitigation recommendations; Execute phishing and spear phishing campaigns; Develop tactics, techniques and procedures for network penetration and data exfiltration; Candidate should be familiar with operating in the network, pivoting, gathering information, etc., as well as modifying existing code and building their own scripts and tools; Document identified vulnerabilities; assist with remediation activities and risk mitigation / management activities by helping to weigh the threat to systems posed by the presence of hostile entities; Working knowledge of penetration testing tools, tactics, techniques, and procedures; Performing assessments of systems and networks to identify where those systems/networks are most vulnerable to hostile cyber entities; Ability to execute reconnaissance commands and analyze output across Windows and Linux platforms; Working knowledge of TCP/IP networking, enterprise network architectures, and systems engineering concepts; Ability to develop custom code in one or more of the following languages: Perl, Python, Java, Ruby, Powershell, or C.

Certifications: Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Requires a minimum of Two (2) years of penetration testing experience.

2. Commercial Job Title: Penetration Tester 2

Functional Responsibility: The Penetration Tester 2 supports the design and execution of penetration testing activities including overall penetration testing strategy, internal and external attack plans, identification of vulnerabilities, execution of exploits, and development of final reports.

Develop custom code to penetrate networks and system defenses to include development of malware, root kits and remote access tools; Develop and execute phishing and spear phishing campaigns; Responsible for identifying and diagnosing systems by expert use of commercial off the shelf and open source resources; Perform Open Source Intelligence (OSINT) campaigns in advance and during penetration testing activities; Conduct open source research on target sites and personnel to include use of pre-texting; Working knowledge of penetration testing tools, tactics, techniques, and procedures; Track remediation progress and provide management with routine progress updates; Ability to recommend and execute reconnaissance commands, and analyze output across Windows and Linux platforms; Strong working knowledge of TCP/IP networking, enterprise network architectures, and systems engineering concepts; Ability to develop custom code in one or more of the following languages: Perl, Python, Java, Ruby, Powershell, or C.

Certifications: Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: At least Five (5) years of penetration testing experience.
3. **Commercial Job Title: Penetration Tester 3**

**Functional Responsibility:** The Penetration Tester 3 leads penetration testing activities and develops the strategy for all phases of activity including reconnaissance, attack planning, exfiltration, and reporting. The Penetration Testing Analyst 3 directs development and execution of the penetration testing effort and associated utilities and execution of scripts.

Diagnose new and emerging vulnerabilities and assist with creation of detection capabilities for Computer Network Defense infrastructure; Maintain knowledge of applicable penetration testing policies, regulations, and compliance requirements; Provide "Lessons Learned" reports for penetration testing events to improve the security posture of supported networks; Conduct open source research on target sites and personnel to include use of pre-texting; Performing assessments of systems and networks to identify where those systems/networks are most vulnerable to hostile cyber entities; Working knowledge of penetration testing tools, tactics, techniques, and procedures; Ability to develop custom code in one or more of the following languages: Perl, Python, Java, Ruby, Powershell, or C; Expert level knowledge of TCP/IP networking, enterprise network architectures, and systems engineering concepts; Ability to identify and execute reconnaissance commands and analyze output across Windows and Linux platforms

**Certifications:** Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**General Experience:** At least Seven (7) years of penetration testing experience.

4. **Commercial Job Title: Incident Responder 1**

**Functional Responsibility:** The Incident Responder 1 role supports evidence collection, identification of exploits, and conducts analysis in support of overall incident response activities.

Implement use of incident response processes to conduct forensic investigations; Provide corrective action recommendations to mitigate security incidents per the incident response SOP; Analyze memory dumps, files, and disk images using the available desktop toolset without impacting network/system operations; Security incident/on-site investigations to verify the scope of a security breach, identify mitigating strategies, and validate mitigations; Hands-on experience using forensic software to investigate, analyze, and catalog incident data; Validate suspicious events or reports and determine if the event constitutes an incident; In depth technical expertise with packet analysis; Analysis of volatile memory dumps, files and full disk images; Develop and maintain an Incident Response Program SOP for incident handling, reporting, and response procedures

**Certifications:** Must have Security+ and at least one of the following applicable incident response certifications: GCIH, GCIA, or CEH.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** At least Two (2) years of incident response experience.
5. **Commercial Job Title: Incident Responder 2**

**Functional Responsibility:** The Incident Responder 2 role develops technical solutions to collect evidence, conducts analysis to determine vulnerabilities, identifies infiltrated data, and develops investigation reports.

Provide incident analysis, forensics, reverse engineering, and fusion reporting to leadership, customers, and appropriate agencies on current and emerging threats, as well as indications and warnings (I&W); Coordinate development and implementation of courses of action (COAs) focusing on containment, eradication, and recovery; Implement use of incident response processes to conduct forensic investigations; Provide network intrusion detection and monitoring, correlation analysis, incident response and support for network security operations; Analyze memory dumps, files, and disk images using the available desktop toolset without impacting network/system operations; Security incident/on-site investigations to verify the scope of a security breach, identify mitigating strategies, and validate mitigations; Hands-on experience using forensic software to investigate, analyze, and catalog incident data; Validate suspicious events or reports and determine if the event constitutes an incident; In depth technical expertise with packet analysis; Analysis of volatile memory dumps, files and full disk images; Preparation and submission of formal management reports citing assessment findings and corrective action; Experience with Security Information Event Management (SIEM) and analytical tools

**Certifications:** Must have Security+ and at least one of the following applicable incident response certifications: GCIH, GCIA, or CEH.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline or equivalent work experience.

**Experience:** At least Five (5) years of incident response experience.

6. **Commercial Job Title: Incident Responder 3**

**Functional Responsibility:** The Incident Responder 3 role leads incident response teams and on-site activities. This role will identify, isolate, investigate, inform, and implement measures to detect and protect data across a wide spectrum of source types and locations.

Provide guidance and oversight for performing forensic investigations on computer systems with detailed documentation of procedures, proper evidence handling, and duplicable investigative results; Provide research support for evaluating systems with suspected compromises and conduct all official investigations; Ensures the acquisition and preservation of data required for tactical analysis, strategic analysis, and/or Counter Intelligence (CI) or Law Enforcement (LE) investigations; Liaise with law enforcement/counter intelligence organizations based on the nature of the incident; Analyze memory dumps, files, and disk images using the available desktop toolset without impacting network/system operations; Security incident/on-site investigations to verify the scope of a security breach, identify mitigating strategies, and validate mitigations; Hands-on experience using forensic software to investigate, analyze, and catalog incident data; Validate suspicious events or reports and determine if the event constitutes an incident; In depth technical expertise with packet analysis; Analysis of volatile memory dumps, files and full disk images; Preparation and submission of formal management reports citing assessment findings and corrective action; Experience with Security Information Event Management (SIEM) and analytical tools; Provide coordination of significant incidents with agency and department level organizations and supported entities to ensure proper analysis is performed and timely and accurate reporting of the incident is affected.

**Certifications:** Must have Security+ and at least one of the following applicable incident response certifications: GCIH, GCIA, or CEH.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline or equivalent work experience.

**Experience:** Seven (7) years of incident response experience.
7. **Commercial Job Title: Cyber Hunt Threat Analyst 1**

**Functional Responsibility:** The Cyber Hunt Threat Analyst 1 uses triage indicators and Real-Time Events to effectively conduct initial analysis and assess the severity of reported events.

Perform daily review of cyber threat warnings, bulletins, alerts, and incident reporting documentation and databases produced by industry and government; Develop indicators of compromise based on known threat information; Interface with cybersecurity teams such as Incident Response, Vulnerability Analysis and Penetration Testing to achieve project objectives; Analyzes relevant cyber security event data for attack indicators and breaches that may yield detection/prevention content; Maintains knowledge of adversary activities, including intrusion set tactics, techniques and procedures (TTP); Maintains situational awareness and reports on advanced threats, including Advanced Persistent Threat (APT) and Focused Operations (FO) incidents; Experience with multiple programming languages; Maintain Standard Operating Procedures documentation; Strong ability to solve problems using a logical approach and deductive reasoning; Strong working knowledge of network concepts and devices including routers, switches, firewalls, IDS/IPS, etc.; Strong technical writing ability to support report development.

**Certifications:** Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

**Experience:** Two (2) years of cyber hunt threat analysis experience.

8. **Commercial Job Title: Cyber Hunt Threat Analyst 2**

**Functional Responsibility:** The Cyber Hunt Threat Analyst 2 implements triage indicators for incident detection and response processes, such as outbound server communication for web traffic, startup programs, and outbound traffic over TCP/UDP ports. The Cyber Hunt Threat Analyst 2 identifies trends and patterns associated with triage indicators.

Perform detailed analysis of log and threat data; Conducts research on emerging security threats; Provides correlation and trending of cyber incident activity; Produces data to support correlation and trending of cyber incident activity; Develop and analyze correlation and trending of cyber incident activity; Develop indicators of compromise based on known threat information; Interface with cybersecurity teams such as Incident Response, Vulnerability Analysis and Penetration Testing to achieve project objectives; Analyzes relevant cyber security event data for attack indicators and breaches that may yield detection/prevention content; Maintains knowledge of adversary activities, including intrusion set tactics, techniques and procedures (TTP); Maintains situational awareness and reports on advanced threats, including Advanced Persistent Threat (APT) and Focused Operations (FO) incidents; Experience with multiple programming languages; Strong ability to solve problems using a logical approach and deductive reasoning; Strong working knowledge of network concepts and devices including routers, switches, firewalls, IDS/IPS, etc.; Ability to write automated scripts or modify existing scripts across multiple programming languages; Implement countermeasures, coordinate response actions, and take steps to contain/isolate threats.

**Certifications:** Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.
**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

**Experience:** Five (5) years of cyber hunt threat analysis experience.

---

9. **Commercial Job Title:** Cyber Hunt Threat Analyst 3

**Functional Responsibility:** The Cyber Hunt Threat Analyst 3 performs cyber intelligence gathering and threat analysis of threats, including nation-state sponsored threats for a large organization. Actively provides in-depth incident analysis. Evaluates security incidents and performs research. Monitors, analyzes and correlates network traffic utilizing the latest in security tools and technology.

Reviews threat data from various sources; coordinates with federal leadership, as well as government agencies to provide reporting and situational awareness; Implementation of countermeasures, remediation compliance, mitigation actions, and ticket closure; Provides thought leadership on emerging security threats and countermeasures; Identifies sources of research on emerging security threats; Communicates events to agencies regarding intrusions and compromises to network infrastructure, applications and operating systems; assists with implementation of countermeasures and mitigating controls; Prepares cyber threat assessments based on threat analysis, coordinates cyber threat tracking with other organizations and the government; assists in developing reports, briefings and assessments to facilitate the understanding of cyber threats; Syslog analysis, network traffic analysis, entry vector analysis, malware analysis, event correlation, damage assessments, forensic analysis and updated reporting; Expert level network packet capture traffic (PCAP) and network traffic flow analysis; Ability to reverse engineer malware and other identified software used to exploit networks and systems; In-depth knowledge of malware and memory analysis; Expert level knowledge of Windows operating system architecture including but not limited to: kernel, registry, file system, APIs.

**Certifications:** Must have Security+ and at least one of the following applicable certifications: CCNP, CCIE, CISSP, GCIA, GCNA, GCIH, GPEN, GCFW, CISA, CISM or ACSA.

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

**Experience:** Seven (7) years of cyber hunt threat analysis experience.

---

10. **Commercial Job Title:** Risk and Vulnerability Assessment Analyst 1

**Functional Responsibility:** The Risk and Vulnerability Assessment Analyst 1 supports the development of security documentation to complete risk management and vulnerability assessment reports. Initiate security documents and conduct interviews with system administrators and application developers to capture required information.

Develop Security Assessment Plans and perform reviews of technical sections of security documentation including architecture diagrams and hardware/ software; Conduct quality assurance reviews of all security documentation deliverables; Developing system authorization packages Expert level proficiency in Microsoft Word; Development of security documentation including but not limited to Security Assessment Report, Security Assessment Plan, and supporting assessment boundary documentation; Experience developing and completing system authorization packages; Working knowledge of 800-53 security controls, control families, and control tailoring; FISMA Audits; Working knowledge of the Risk Management Framework 6 step process.
Certifications: Must have at least one of the following applicable certifications: CISSP, CAP, CISM, CISA, CASP.

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

Experience: Two (2) years of risk management and vulnerability assessment experience.

11. Commercial Job Title: Risk and Vulnerability Assessment Analyst 2

Functional Responsibility: The Risk and Vulnerability Assessment Analyst 2 maintains direct responsibility for leading and completing technical engineering tasks on the project timeline and maintains responsibility for assessment boundary definition, hardware and software inventories, vulnerability scanning, vulnerability analysis, technical input to security documentation, and technical issue resolution.

Conducting vulnerability scans using commercial available tools to scan networks including general vulnerability scanners, database scanners, applications scanners and source code scanners; Review vulnerability scans to identify false positives, mitigation strategies, and system fixes; Interface with technical engineering counterparts to capture information required for security documentation; Ability to establish assessment boundaries using network diagrams, hardware/software list, and technical collaboration sessions; Development of detailed network diagrams using Microsoft Visio; Experience developing and completing system authorization packages; FISMA Audits; Working knowledge of the Risk Management Framework 6 step process; Working knowledge of 800-53 security controls, control families, and control tailoring.

Certifications: Must have at least one of the following applicable certifications: CISSP, CAP, CISM, CISA, CASP.

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

Experience: Five (5) years of risk management and vulnerability assessment experience.

12. Commercial Job Title: Risk and Vulnerability Assessment Analyst 3

Functional Responsibility: The Risk and Vulnerability Assessment Analyst 3 maintains direct responsibility for leading and completing risk management and vulnerability assessment tasks. The Risk Management Analyst 3 leads security control tailoring requirements, identifies applicable security standards, and recommends appropriate vulnerability assessment scanning policies. The Risk and Vulnerability Assessment Analyst 3 leads the development and review of project deliverables.

Maintain direct responsibility for leading and completing tasks associated with security control assessments and developing security documentation; Track the progress of assessment teams by proactively identifying the completion of timeline milestones; Enterprise architecture analysis; In Depth knowledge of 800-53 security controls. Experience with most current versions of 800-53 security controls highly desired; Experience with tailoring 800-53 security controls; Experience developing processes to support the Risk Management Framework; Experience developing and completing system authorization packages; Development of reports in support of FISMA compliance; Strong working knowledge of the Risk Management Framework 6 step process in Federal and DoD environments.

Certifications: Must have at least one of the following applicable certifications: CISSP, CAP, CISM, CISA. PMP certification also highly desired.
Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience

Experience: Seven (7) years of risk management and vulnerability assessment experience.

13. Commercial Job Title: Cybersecurity Engineer 1

Functional Responsibility: The Cybersecurity Engineer 1 maintains expertise in cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security. The Cybersecurity Engineer provides design, engineering, and administration support to cybersecurity tool sets for enterprise organizations. The Cybersecurity Engineer integrates COTS, GOTS, and custom products to achieve working solutions for enterprise networks.

Documentation support includes network diagrams, data flow diagrams, security control documentation, system authorization packages, Work Instructions, Concept of Operations (CONOPS) and Standard Operating Procedures (SOPs). Candidate should be familiar with building their own scripts and tools; Document identified vulnerabilities; assist with remediation activities and risk mitigation/defense in depth / management activities by helping to weigh the threat to systems posed by the presence of hostile entities; Working knowledge of cybersecurity tools, tactics, techniques, and procedures; Performing assessments of systems and networks to identify where those systems/networks are most vulnerable to hostile cyber entities; Ability to execute network engineering commands and analyze output across Windows and Linux platforms; Working knowledge of TCP/IP networking, enterprise network architectures, and systems engineering concepts; Ability to develop automation scripts to make use of REST APIs in one or more of the following languages: Python, PowerShell, JSON, XML, or Postman.

Certifications: Must have at least one of the following applicable certifications: Security +CE, Network +CE, A +CE, CCNA, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: A minimum of one (1) year of experience in cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security.

14. Commercial Job Title: Cybersecurity Engineer 2

Functional Responsibility: The Cybersecurity Engineer 2 maintains expertise in multiple cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security. The Cybersecurity Engineer 2 leads design, engineering, and administration support to cybersecurity tool sets for enterprise organizations. The Cybersecurity Engineer integrates COTS, GOTS, and custom products to achieve working solutions for enterprise networks.

Documentation support includes network diagrams, data flow diagrams, security control documentation, system authorization packages, Work Instructions, Concept of Operations (CONOPS) and Standard Operating Procedures (SOPs). The Cybersecurity Engineer 2 builds their own automation scripts and tools; Document identified vulnerabilities; assist with remediation activities and risk mitigation / management activities by helping to weigh the threat to systems posed by the presence of hostile entities; Advanced knowledge of cybersecurity tools, tactics, techniques, and procedures; Lead assessments of systems and networks to identify where those systems/networks are most vulnerable to hostile cyber entities; Efficient command of network engineering commands and analyze output across Windows and Linux platforms; Strong knowledge of TCP/IP networking,
enterprise network architectures, and systems engineering concepts; Ability to develop automation scripts to make use of REST APIs in one or more of the following languages: Python, PowerShell, JSON, XML, or Postman.

Certifications: Must have at least one of the following applicable certifications: CASP, CAP, Security +CE, CCNA Security, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Three (3) years of experience in multiple cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security.

15. Commercial Job Title: Cybersecurity Engineer 3

Functional Responsibility: The Cybersecurity Engineer 3 maintains expertise across all cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security. The Cybersecurity Engineer 3 leads teams in design, engineering, and administration support to cybersecurity tool sets for enterprise organizations. The Cybersecurity Engineer 3 leads teams and major integration projects for COTS, GOTS, and custom products to achieve working solutions for enterprise networks.

Documentation support includes network diagrams, data flow diagrams, security control documentation, system authorization packages, Work Instructions, Concept of Operations (CONOPS) and Standard Operating Procedures (SOPs). The Cybersecurity Engineer 3 builds their own automation scripts and tools; Document identified vulnerabilities; assist with remediation activities and risk mitigation / management activities by helping to weigh the threat to systems posed by the presence of hostile entities; Expert knowledge of cybersecurity tools, tactics, techniques, and procedures; Lead teams for assessments of systems and networks to identify where those systems/networks are most vulnerable to hostile cyber entities; Expert command of network engineering commands and analyze output across Windows and Linux platforms; Strong knowledge of TCP/IP networking, enterprise network architectures, and systems engineering concepts; Ability to develop automation scripts to make use of REST APIs in one or more of the following languages: Python, PowerShell, JSON, XML, or Postman.

Certifications: Must have at least one of the following applicable certifications: CISM, CSSP, CISA, CASP, CAP, CCNP Security, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Five (5) years of experience across all cybersecurity engineering baseline disciplines including vulnerability scanning, firewalls, intrusion detection, packet capture, and endpoint security.

16. Commercial Job Title: Cybersecurity Subject Matter Expert 1

Functional Responsibility: The Cybersecurity Subject Matter Expert 1 role maintains specialized expertise in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services. Cybersecurity technology area examples include endpoint protection, intrusion detection and prevention, policy, Security Information Event Management (SIEM), packet capture, vulnerability scanning, and threat intelligence. This role contributes to a cybersecurity team to provide subject matter expert support across multiple disciplines including design, implementation, operation, governance, policy, oversight, operation, and more.
Implement use of Concepts of Operations, Standard Operating Procedures, and Work Instructions to advance cybersecurity risk management, compliance, and operational task areas; Provide corrective action recommendations to mitigate security incidents per the incident response SOP; Analyze data sets and output from cybersecurity tools using the available desktop toolset without impacting network/system operations; Hands-on experience using specialized IT systems and cybersecurity tools to promote compliance and defense-in-depth strategies.

Certifications: Must have at least one of the following applicable certifications: Security +CE, Network +CE, A +CE, CCNA, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: One (1) year of specialized experience in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services.

17. Commercial Job Title: Cybersecurity Subject Matter Expert 2

Functional Responsibility: The Cybersecurity Subject Matter Expert 2 role maintains advanced expertise in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services. Cybersecurity technology area examples include endpoint protection, Security Information Event Management (SIEM), intrusion detection and prevention, policy, packet capture, vulnerability scanning, and threat intelligence. This role contributes to a cybersecurity team to provide subject matter expert support across multiple disciplines including design, implementation, operation, governance, policy, oversight, operation, and more.

Leads and develops use of Concepts of Operations, Standard Operating Procedures, and Work Instructions to advance cybersecurity risk management, compliance, and operational task areas; Provide corrective action recommendations to mitigate security incidents per the incident response SOP; Analyze data sets and output from cybersecurity tools using the available desktop toolset without impacting network/system operations; Hands-on experience using specialized IT systems and cybersecurity tools to promote compliance and defense-in-depth strategies.

Certifications: Must have at least one of the following applicable certifications: CASP, CAP, Security+ CE, CCNA Security, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Three (3) years of advanced experience in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services.

18. Commercial Job Title: Cybersecurity Subject Matter Expert 3

Functional Responsibility: The Cybersecurity Subject Matter Expert 3 role maintains expert level experience in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services. Cybersecurity technology area examples include endpoint protection, Security Information Event Management (SIEM), intrusion detection and prevention, policy, packet capture, vulnerability scanning, and threat intelligence. This role contributes to a cybersecurity team to provide subject
matter expert support across multiple disciplines including design, implementation, operation, governance, policy, oversight, operation, and more.

Guides, leads and develops use of Concepts of Operations, Standard Operating Procedures, and Work Instructions to advance cybersecurity risk management, compliance, and operational task areas; Provide corrective action recommendations to mitigate security incidents per the incident response SOP; Analyze data sets and output from cybersecurity tools using the available desktop toolset without impacting network/system operations; Hands-on experience using specialized IT systems and cybersecurity tools to promote compliance and defense-in-depth strategies.

**Certifications:** Must have at least one of the following applicable certifications: CISM, CSSP, CISA, CASP, CAP, CCNP Security, SSCP

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** Five (5) years of experience in a cybersecurity vertical or technology area. Cybersecurity vertical examples include healthcare, defense, transportation, and professional services.

---

19. **Commercial Job Title: SOC Analyst 1**

**Functional Responsibility:** The SOC Analyst 1 uses triage indicators and Real-Time Events to effectively conduct initial analysis and assess the severity of reported events. Perform daily review of cyber threat warnings, bulletins, alerts, and incident reporting documentation and databases produced by industry and government; Develop indicators of compromise based on known threat information; Interface with cybersecurity teams such as Incident Response, Vulnerability Analysis and Penetration Testing to achieve project objectives.

Analyzes relevant cyber security event data for attack indicators and breaches that may yield detection/prevention content; Maintains knowledge of adversary activities, including intrusion set tactics, techniques and procedures (TTP); Maintains situational awareness and reports on advanced threats, including Advanced Persistent Threat (APT) and Focused Operations (FO) incidents; Experience with multiple programming languages; Maintain Standard Operating Procedures documentation; Strong ability to solve problems using a logical approach and deductive reasoning; Strong working knowledge of network concepts and devices including routers, switches, firewalls, IDS/IPS, etc.; Strong technical writing ability to support report development.

**Certifications:** Must have at least one of the following applicable certifications: Security +CE, Network +CE, A +CE, CCNA, SSCP

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** A minimum of one (1) year of experience using triage indicators and Real-Time Events to effectively conduct initial analysis and assess the severity of reported events.

---

20. **Commercial Job Title: SOC Analyst 2**

**Functional Responsibility:** The SOC Analyst 2 implements triage indicators for incident detection and response processes, such as outbound server communication for web traffic, startup programs, and outbound traffic over TCP/UDP ports. The SOC Analyst 2 identifies trends and patterns associated with triage indicators.
Detailed analysis of log and threat data; Conducts research on emerging security threats; Provides correlation and trending of cyber incident activity; Produces data to support correlation and trending of cyber incident activity; Develop and analyze correlation and trending of cyber incident activity; Develop indicators of compromise based on known threat information; Interface with cybersecurity teams such as Incident Response, Vulnerability Analysis and Penetration Testing to achieve project objectives; Analyzes relevant cyber security event data for attack indicators and breaches that may yield detection/prevention content; Maintains knowledge of adversary activities, including intrusion set tactics, techniques and procedures (TTP); Maintains situational awareness and reports on advanced threats, including Advanced Persistent Threat (APT) and Focused Operations (FO) incidents; Experience with multiple programming languages; Strong ability to solve problems using a logical approach and deductive reasoning; Strong working knowledge of network concepts and devices including routers, switches, firewalls, IDS/IPS, etc.; Ability to write automated scripts or modify existing scripts across multiple programming languages; Implement countermeasures, coordinate response actions, and take steps to contain/isolate threats.

Certifications: Must have at least one of the following applicable certifications: CISM, CSSP, CISA, CASP, CAP, CCNP Security, SSCP

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Five (5) years of experience implementing triage indicators for incident detection and response processes, to include identifying trends and patterns associated with triage indicators.

21. Commercial Job Title: SOC Analyst 3

Functional Responsibility: The SOC Analyst 3 performs cyber intelligence gathering and threat analysis of threats, including nation-state sponsored threats for a large organization. Actively provides in-depth incident analysis. Evaluates security incidents and performs research. Monitors, analyzes and correlates network traffic utilizing the latest in security tools and technology.

Reviews threat data from various sources; coordinates with federal leadership, as well as government agencies to provide reporting and situational awareness; Implementation of countermeasures, remediation compliance, mitigation actions, and ticket closure; Provides thought leadership on emerging security threats and countermeasures; Identifies sources of research on emerging security threats; Communicates events to agencies regarding intrusions and compromises to network infrastructure, applications and operating systems; assists with implementation of counter-measures and mitigating controls; Prepares cyber threat assessments based on threat analysis, coordinates cyber threat tracking with other organizations and the government; assists in developing reports, briefings and assessments to facilitate the understanding of cyber threats; Syslog analysis, network traffic analysis, entry vector analysis, malware analysis, event correlation, damage assessments, forensic analysis and updated reporting; Expert level network packet capture traffic (PCAP) and network traffic flow analysis; Ability to reverse engineer malware and other identified software used to exploit networks and systems; In-depth knowledge of malware and memory analysis; Expert level knowledge of Windows operating system architecture including but not limited to: kernel, registry, file system, APIs.

Certifications: Must have at least one of the following applicable certifications: CISSP, CISM, GCIH, GSLC, CCNP Security

Education: Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

Experience: Seven (7) years of experience performing cyber intelligence gathering and threat analysis of threats, including nation-state sponsored threats for a large organization.
22. Commercial Job Title: Task Lead

**Functional Responsibility:** The Task Lead maintains direct responsibility for leading specialized cybersecurity teams to complete engineering and program support tasks on the project timeline. Maintains expertise in one or more cybersecurity frameworks.

Engages with team members and leads interface across cybersecurity teams to achieve objectives. The Task Lead manages one or more task areas of a cybersecurity program and implements cross-training and knowledge management to develop Standard Operating Procedures and Concepts of Operations (CONOPS).

**Certifications:** Must have at least one of the following applicable certifications: CISM, CSSP, CISA, CASP, CAP, CCNP Security, SSCP

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** Five (5) years of experience leading specialized cybersecurity teams to complete engineering and program support tasks on the project timeline and implementing cybersecurity frameworks within one or more domains.

23. Commercial Job Title: Program Manager

**Functional Responsibility:** Provide effective leadership, oversight, development and program management over programs, projects and Task Orders. Develop and establish Standard Operating Procedures and implement policies and procedures in accordance with government directives. Work with the government Program Office to identify funding source and develop and maintain program execution budgets. Establish strategic goals and objectives and report program performance and budget actual against plan to the corporate Program Management Office (PMO). Manage innovation initiatives and maintain direct responsible for the reduction of cost and time associated with process improvements.

Manages the technical direction of programs and projects in accordance with corporate policies and procedures and provide cost, schedule, risk, quality assurance and control of information to the Government Program Office. The Program Manager (PM) reports to the PMO and will have overall responsibility for the Quality Assurance (QA) and Quality Control (QC) for the work, deliverables, processes, and daily operations of the program. Performs assessments and evaluations of program(s) and process components; validate results, report discrepancies; and follows through to ensure that all issues are resolved on a timely basis.

The PM will be responsible for the effective management of all tasks associated with a program and will maintain responsible for ensuring customer satisfaction and oversees technology and resource allocation. The PM will also participate in pre-award/post award and transition planning and organizing to ensure that each task is perform efficiently, accurately, on time, and in compliance with the contract requirements.

**Certifications:** Must have at least one of the following applicable certifications: CISSP, CISM, GCIH, GSLC, CCNP Security

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** Ten (10) years of effective leadership, oversight, development and program management over programs, projects, and Task Orders.
24. **Commercial Job Title: Healthcare Cybersecurity Specialist**

**Functional Responsibility:** Specialized expertise in healthcare networks, medical devices, clinical systems, research laboratories, administrative offices, hospitals, billing, fraud prevention, policy, governance, frameworks, or other Healthcare IT discipline.

Develop communication products, summaries, executive reporting, technical diagrams, and other materials necessary to communicate Healthcare Cybersecurity activities to internal and external stakeholders. Develop, author, and revise policy documents, MOU/MOAs, agreements, and other supporting documentation to facilitate the collaboration, sharing and communications mission. Develop and facilitate Concept of Operations (CONOPS), Standard Operating Procedures (SOPs), policies, memos, and supporting documentation to support cybersecurity collaboration and knowledge sharing. Discern trends and patterns from threat feed data to support risk management decisions.

**Certifications:** Must have at least one of the following applicable certifications: CISSP, CISM, GCIH, GSIC, PMP, ISO, ITIL

**Education:** Bachelor’s degree in Computer Science, Information Systems, or other related scientific or technical discipline, or equivalent work experience.

**Experience:** Ten (10) years of experience in healthcare networks, medical devices, clinical systems, research laboratories, administrative offices, hospitals, billing, fraud prevention, policy, governance, frameworks, or other Healthcare IT discipline.

---

54151HEAL GSA Labor Category Descriptions

1. **Commercial Job Title: Health IT Program Manager (PM)**

**Functional Responsibility:** Provide effective leadership, oversight, development and program management over Health IT programs, projects, and Task Orders. Develop and establish Standard Operating Procedures and implement policies and procedures in accordance with government directives. Work with the government Program Office to identify funding source and develop and maintain program execution budgets. Establish strategic goals and objectives and report program performance and budget actual against plan to the corporate Program Management Office (PMO). Manage innovation initiatives and maintain direct responsibility for the reduction of cost and time associated with process improvements.

Manages the technical direction of Health IT programs and projects in accordance with corporate policies and procedures and provide cost, schedule, risk, quality assurance and control of information to the Government Program Office. The Health IT PM reports to the PMO and will have overall responsibility for the Quality Assurance (QA) and Quality Control (QC) for the work, deliverables, processes, and daily operations of the program. Performs assessments and evaluations of program(s) and process components; validate results, report discrepancies; and follows through to ensure that all issues are resolved on a timely basis.

The Health IT PM will be responsible for the effective management of all tasks associated with a program and will maintain responsible for ensuring customer satisfaction and oversees technology and resource allocation. The PM will also participate in pre-award/post award and transition planning and organizing to ensure that each task is perform efficiently, accurately, on time, and in compliance with the contract requirements. The Health IT PM will coordinate when applicable with the government Program Manager and the Contracting Officer Representative (COR) to ensure that the program is manage consistently with overall contract requirements and will ensure timely and accurate submission of invoices.

**Education:** Bachelor’s Degree in Information System or Business Finance Management or Computer
Sciences or related discipline.

**Certifications:** Project Management Professional (PMP).

**Experience:** Requires a minimum of 15 years of technical engineering experience and 5 or more years of program management experience in assigned business area.

---

2. **Commercial Job Title: Health IT Subject Matter Expert 5 (SME5)**

**Functional Responsibility:** The Health IT SME5 is responsible for the management of a team of engineers, analysts, and project contributors. He/She is directly responsible for the analysis and development of technical engineering documentation that is delivered to the government for approval. The SME5 is required to supervise the work of the SME4, SME3, and SME2 to ensure that the customer Standard OPERATING Procedures are being followed. The SME5 is also responsible for the creation of Configuration Management documentation. The SME5 also provides technical leadership and guidance to the SME4 and SME3 during the implementation of solutions for the customer’s network. He/She is required to verify that all devices are under the configuration management process. In addition, the SME5 is responsible for leading the weekly team meetings with the customer and providing status reports to senior management.

To carry-out the Health IT engineering and management responsibilities identified above, The SME5 must exhibit the experience and ability to provide enterprise-wide technical management and direction for problem definition, analysis and requirements development and implementation for very complex IT systems in the subject matter area. Additionally, this individual has the ability to provide workable recommendations and advice to client executive management on emerging technology, system improvements, optimization and maintenance in the following areas: Health IT Information Systems Architecture, Health IT Automation, Health IT Telecommunications, Health IT Networking, Communication Protocols, Software, Electronic Email, Modeling and Simulation, Data Storage and Retrieval. The SME5 must have the required Health IT experience and ability to provide technical management and direction for problem definition, analysis and requirements development and implementation for complex IT systems in the subject matter area.

**Education:** Bachelor’s Degree in Computer Science or related field; a Master Degree in Computer Science of Engineering is a preferred and a certification in Certified Information Systems Security Professional (CISSP) or equivalent specialized certification in technical discipline is required.

**Experience:** At least ten (10) years of progressive applied technical experience with complex Enterprise systems and Networks.

---

3. **Commercial Job Title: Health IT Subject Matter Expert 4 (SME4)**

**Functional Responsibility:** The Health IT SME4 reports to a Health IT Program Manager or SME5 as a member of the technical team. He/She is responsible for providing Health IT technical/engineering assistance to the project. The SME4 is required to provide technical input to the configuration management process. The SME4 must exhibit the technical ability and know-how to conduct technical analysis using automated tools and checklist to develop and implement solutions for large enterprise networks. The Health IT SME4 must have technical knowledge of database management systems and applications. He/She must have the ability to effectively communicate network vulnerabilities and required safeguards to the customer’s engineering staff. In addition, the SME4 is responsible for uploading network scan results to the automated system and to interface with the customer to communicate, interpret and analyze technical results.

This individual exhibits the ability to assist the project team in providing workable recommendations and advice on system improvements, optimization, and maintenance in the following areas: Health IT Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.
Education: Bachelor’s Degree in Computer Science or related field is required; a certification in an IT technical discipline is required.

General Experience: At least seven (7) years of progressive applied technical experience with complex IT network.

4. **Commercial Job Title: Health IT Subject Matter Expert 3 (SME3)**

   **Functional Responsibility:** The Health IT SME3 reports to a Health IT Program Manager or SME5 and is required to have experience in conducting technical reviews of system documentation and providing quality assurance on all of the configuration management documentation package. SME3 is also responsible for working under the technical supervision of the SME4 and SME5 to assist with the assessment of the enterprise environment. The Health IT SME3 duties entail that he or she carry-out and completes technical tasks requiring a lower level of technical expertise and is responsible for the preparation of the configuration documentation. The SME3 must have the ability to effectively communicate the customer’s requirements to the SME4 and SME5 and make recommendations and advise on organization-wide process improvements.

   In summary, this individual in conjunction with Health IT directives laid out by SME4 and SME5 has the ability to coordinate and manage the preparation of analysis, evaluations, and recommendations for proper implementation of programs and systems specifications in the following specialties: Health IT Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.

   **Education:** Bachelor’s Degree in Computer Science or related field; an associate level certification is required from CompTIA or equivalent recognized organization.

   **Experience:** At least three (3) years of progressive applied technical experience with Health IT systems.

5. **Commercial Job Title: Health IT Subject Matter Expert 2 (SME2)**

   **Functional Responsibility:** Defines the problems and analyzes and develops plans and requirements in the Health IT subject matter area for simple to moderately complex systems. Consults directly with client to define need, obtains required data, and analyzes data to advise on or recommend solution. Provides technical expertise in a specific technical area, typically translating raw data into concise documentation for technical higher level Health IT SME’s and complimentary non-technical staff. The SME2 reports directly to the Health IT SME 4 and SME5, providing overall quality assurance for the configuration management package. Duties also entail that this individual provides technical review, technical writing, and generates summaries, reports, and presentations, such as technology assessments and program audits. Individual has demonstrated competence using Health IT data from project management tools - simultaneously planning and managing with higher level SME team the transition of highly technical projects from planning to execution of tasks.

   In summary, this individual has ability, in conjunction with our team of subject matter experts, to coordinate and manage the preparation of analysis, evaluations, and recommendations for proper implementation of Health IT programs and systems specifications in the following specialties: Health IT Information Systems Architecture; Networking; Telecommunications; Automation; Communications Protocols; Risk Management/Electronic Analysis; Software; Life-Cycle Management; Software Development Methodologies; Modeling and Simulation.

   **Education:** Bachelor’s Degree in Computer Science, Business, or related field is required; an associate level certification is required from CompTIA or equivalent recognized organization.

   **Experience:** At least two (2) years of progressive applied technical experience with simple to moderately complex Health IT systems.
6. **Commercial Job Title: Health IT Help Desk Specialist (Senior Level)**

**Functional Responsibility:** Under general supervision provides tier 2 support to end users for Health IT PC, service, mainframe applications, and hardware. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends system modifications to reduce user problems. Maintains currency and highest-level technical skills in field of expertise. Demonstrated ability to assist in the use of software and hardware, servers, printers, network components, and other peripheral components. Ability to conduct component level diagnostics.

Demonstrated ability to assist in the use of a variety of business software and operating systems. Ability to develop and maintain documentation for procedures and processes, as well as, maintenance logs and equipment databases. Ability to effectively communicate orally and in writing. Ability to teach hardware concepts to customers with little or no background in computers.

**Education:** Associate degree or equivalent experience with CompTIA certification.

**Experience:** Six (6) Months of applied Health IT experience.
## CONTRACTOR’S AWARDED GSA PRICING

### 54151S – Awarded GSA Hourly Rates

Network Security Systems Plus, Inc.  
Awarded GSA Hourly Rates  
GSA Authorized Pricelist  
GS-35F-0232X

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Effective Date</strong></td>
<td>2/15/21-2/14/22</td>
<td>2/15/22-2/14/23</td>
<td>2/15/23-2/14/24</td>
<td>2/15/24-2/14/25</td>
<td>2/15/25-2/14/26</td>
</tr>
<tr>
<td>54151S</td>
<td>Program Manager</td>
<td>$165.63</td>
<td>$165.63</td>
<td>$165.63</td>
<td>$165.63</td>
<td>$165.63</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert 5</td>
<td>$156.94</td>
<td>$156.94</td>
<td>$156.94</td>
<td>$156.94</td>
<td>$156.94</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert 4</td>
<td>$127.16</td>
<td>$127.16</td>
<td>$127.16</td>
<td>$127.16</td>
<td>$127.16</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert 3</td>
<td>$108.23</td>
<td>$108.23</td>
<td>$108.23</td>
<td>$108.23</td>
<td>$108.23</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert 2</td>
<td>$91.99</td>
<td>$91.99</td>
<td>$91.99</td>
<td>$91.99</td>
<td>$91.99</td>
</tr>
<tr>
<td>54151S</td>
<td>Help Desk Specialist (Senior Level)</td>
<td>$57.93</td>
<td>$57.93</td>
<td>$57.93</td>
<td>$57.93</td>
<td>$57.93</td>
</tr>
</tbody>
</table>
# 54151HACS – Awarded GSA Hourly Rates

**Network Security Systems Plus, Inc.**  
Awarded GSA Hourly Rates  
GSA Authorized Pricelist  
GS-35F-0232X

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 1</td>
<td>$82.41</td>
<td>$82.41</td>
<td>$82.41</td>
<td>$82.41</td>
<td>$82.41</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 2</td>
<td>$105.97</td>
<td>$105.97</td>
<td>$105.97</td>
<td>$105.97</td>
<td>$105.97</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 3</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 1</td>
<td>$118.96</td>
<td>$118.96</td>
<td>$118.96</td>
<td>$118.96</td>
<td>$118.96</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 2</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 3</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 1</td>
<td>$122.96</td>
<td>$122.96</td>
<td>$122.96</td>
<td>$122.96</td>
<td>$122.96</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 2</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
<td>$137.24</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 3</td>
<td>$144.34</td>
<td>$144.34</td>
<td>$144.34</td>
<td>$144.34</td>
<td>$144.34</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 1</td>
<td>$120.83</td>
<td>$120.83</td>
<td>$120.83</td>
<td>$120.83</td>
<td>$120.83</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 2</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
<td>$127.20</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 3</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
<td>$134.57</td>
</tr>
</tbody>
</table>

**Option Term**

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 1</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 2</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester 3</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 1</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 2</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Responder 3</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 1</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 2</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Hunt Threat Analyst 3</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 1</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 2</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Risk and Vulnerability Assessment Analyst 3</td>
<td>2/15/21 - 2/14/22</td>
<td>2/15/22 - 2/14/23</td>
<td>2/15/23 - 2/14/24</td>
<td>2/15/24 - 2/14/25</td>
<td>2/15/25 - 2/14/26</td>
</tr>
</tbody>
</table>
## 54151HACS – Awarded GSA Hourly Rates

### Network Security Systems Plus, Inc.

**Awarded GSA Hourly Rates**  
**GSA Authorized Pricelist**  
**GS-35F-0232X**

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Engineer 1</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Engineer 2</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Engineer 3</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Subject Matter Expert 2</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cybersecurity Subject Matter Expert 3</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>SOC Analyst 1</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
</tr>
<tr>
<td>54151HACS</td>
<td>SOC Analyst 2</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
</tr>
<tr>
<td>54151HACS</td>
<td>SOC Analyst 3</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Task Lead</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Project Manager</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Healthcare Cybersecurity Specialist</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
</tr>
</tbody>
</table>

**Option Term**

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/15/21-2/14/22</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
<td>$83.32</td>
</tr>
<tr>
<td>2/15/22-2/14/23</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
<td>$97.66</td>
</tr>
<tr>
<td>2/15/23-2/14/24</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
<td>$126.55</td>
</tr>
<tr>
<td>2/15/25-2/14/26</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
<td>$121.07</td>
</tr>
<tr>
<td>2/15/26-2/14/27</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
<td>$106.26</td>
</tr>
<tr>
<td>2/15/27-2/14/28</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
<td>$89.93</td>
</tr>
<tr>
<td>2/15/28-2/14/29</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
<td>$119.26</td>
</tr>
<tr>
<td>2/15/29-2/14/30</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
<td>$126.69</td>
</tr>
<tr>
<td>2/15/30-2/14/31</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
<td>$115.29</td>
</tr>
<tr>
<td>2/14/31-2/14/32</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
<td>$109.45</td>
</tr>
<tr>
<td>2/14/32-2/14/33</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
<td>$147.11</td>
</tr>
</tbody>
</table>
### 54151HEAL – Awarded GSA Hourly Rates

**Network Security Systems Plus, Inc.**  
**Awarded GSA Hourly Rates**  
**GSA Authorized Pricelist**  
**GS-35F-0232X**

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Hourly Rate Year 11</th>
<th>GSA Hourly Rate Year 12</th>
<th>GSA Hourly Rate Year 13</th>
<th>GSA Hourly Rate Year 14</th>
<th>GSA Hourly Rate Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HEAL</td>
<td>Health IT Program Manager</td>
<td>$155.61</td>
<td>$155.61</td>
<td>$155.61</td>
<td>$155.61</td>
<td>$155.61</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Subject Matter Expert 5</td>
<td>$135.59</td>
<td>$135.59</td>
<td>$135.59</td>
<td>$135.59</td>
<td>$135.59</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Subject Matter Expert 4</td>
<td>$111.10</td>
<td>$111.10</td>
<td>$111.10</td>
<td>$111.10</td>
<td>$111.10</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Subject Matter Expert 3</td>
<td>$97.15</td>
<td>$97.15</td>
<td>$97.15</td>
<td>$97.15</td>
<td>$97.15</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Subject Matter Expert 2</td>
<td>$95.18</td>
<td>$95.18</td>
<td>$95.18</td>
<td>$95.18</td>
<td>$95.18</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Help Desk Specialist</td>
<td>$79.99</td>
<td>$79.99</td>
<td>$79.99</td>
<td>$79.99</td>
<td>$79.99</td>
</tr>
</tbody>
</table>

*Effective Date: 2/15/21 - 2/14/22*

2/15/22 - 2/14/23

2/15/23 - 2/14/24

2/15/24 - 2/14/25

2/15/25 - 2/14/26