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

http://www.gsaadvantage.gov

Digital Forensic Services, LLC
9111 Edmonston Road, Suite 205
Greenbelt, MD 20770
PHONE # 410-963-0674
FAX # 301-262-4051

http://www.digitalforensics-usa.com

Contract Number: GS-35F-214DA
Period Covered by Contract: March 7, 2016 through March 6, 2021

General Services Administration
Federal Acquisition Service
1. Awarded Special Item Number(s):

Special Item Number 54151HACS -- HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)

   High Value Asset (HVA) Assessments
   HACS Risk and Vulnerability Assessments (RVA)
   Penetration Testing
   Incident Response
   Cyber Hunt

   FPDS Code D301 IT and Telecom -- Facility Operation and Maintenance
   FPDS Code D302 IT and Telecom -- Systems Development
   FPDS Code D306 IT and Telecom -- Systems Analysis
   FPDS Code D307 IT and Telecom -- IT Strategy and Architecture
   FPDS Code D308 IT and Telecom -- Programming
   FPDS Code D310 IT and Telecom -- Cyber Security and Data Backup
   FPDS Code D311 IT and Telecom -- Data Conversion Services
   FPDS Code D316 IT and Telecom -- Telecommunications Network Management

Special Item Number 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

   FPDS Code D301 IT and Telecom -- Facility Operation and Maintenance
   FPDS Code D302 IT and Telecom -- Systems Development
   FPDS Code D306 IT and Telecom -- Systems Analysis
   FPDS Code D307 IT and Telecom -- IT Strategy and Architecture
   FPDS Code D308 IT and Telecom -- Programming
   FPDS Code D310 IT and Telecom -- Cyber Security and Data Backup
   FPDS Code D311 IT and Telecom -- Data Conversion Services
   FPDS Code D316 IT and Telecom -- Telecommunications Network Management
| SIN 54151S Professional IT Services and, | FPDS Code D301-IT Facility Operation and Maintenance |
| SIN 54151HACS Highly Adaptive Cybersecurity Services (HACS) Subcategories | FPDS Code D302- IT Systems Development Services |
| | FPDS Code D306- IT Systems Analysis Services |
| | FPDS Code D307- Automated Information Systems Design and Integration Services |
| | FPDS Code D308- Programming Services |
| | FPDS Code D310- IT Data Conversion Services |
| | FPDS Code D316- IT Network Management Services |
| | FPDS Code D399- Other Information Technology Services, Not Elsewhere Classified |

**b.** Identification of the lowest priced labor category title and hourly rate awarded under the contract is:

<table>
<thead>
<tr>
<th>Labor Category Title</th>
<th>GSA Hourly Rate/Includes IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Analyst</td>
<td>$81.16</td>
</tr>
</tbody>
</table>

**c.** Labor Category Descriptions of all corresponding labor category titles, general experience, functional responsibility and education are outlined on Pages 14-30 within this pricelist.

2. **Maximum Order:** $500,000 per SIN – For SINs 54151S and 54151 HACS

3. **Minimum Order:** $100.00

4. **Geographic Scope of Coverage:** The Geographic Scope of Coverage is Domestic Delivery. This is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

5. **Quantity Discounts:** None

6. **Volume Discounts:** Additional 1.5% discount for a single task order of $300,000 and over.

7. **Prompt Payment Terms:** 1%-10 days
8. **Government Purchase Cards**: Government Purchase Cards will be accepted however no additional discounts will apply under the contract.

9. **Government Educational Institutional Discounts**: The Government Educational Institutions are offered the same types of discounts and concessions under this contract as all other Government customers.

10. **Foreign Items**: No foreign items are awarded under this contract.

11. **Normal Delivery Terms** – As negotiated between Digital Forensic Services, LLC and the Ordering Activity

   a. **Expedited Delivery Terms**: As Negotiated between Digital Forensic Services, LLC and the Ordering Activity

   b. **Overnight/2-Day Delivery Terms**: As negotiated between Digital Forensic Services, LLC and the Ordering Activity

   c. **Urgent Requirements**: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

12. **FOB Point**: Destination

13. **Ordering Address**: Digital Forensic Services, LLC
    9111 Edmonston Road, Suite 205
    Greenbelt, MD 20770-1546

14. **Payment Address**: Digital Forensic Services, LLC
    9111 Edmonston Road, Suite 205
    Greenbelt, MD 20770-1546

15. **Warranty/Guarantee Provisions**: All services performed under this contract will be guaranteed to completed in a satisfactory workmanlike manner as delineated with this GSA Schedule 70 Schedule Pricelist.

16. **Export Packing Charges**: Export Packing is not offered under this contract.

**List of Participating Dealers**: Digital Forensic Services, LLC does not authorize any participating dealers under this contract.
17. **Environmental Attributes** (e.g., recycled content, energy efficiency, and/or reduced pollutants): Not Applicable

18. **Section 508 Compliance**: Contact Digital Forensic Services, LLC for Section 508 compliance information. The EIT standards can be found at: http://www.section508.gov

19. **Liability For Injury or Damage**: The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

20. **Data Universal Numbering System (DUNS) Number**: 787092332
   a. **Taxpayer Identification Number (TIN)**: 14-1963581
   b. **Business Size**: Small Business Concern
   c. **CAGE Code**: 4L7FO
   d. **Digital Forensic Services, LLC** is currently registered within the System for Award Management (SAM) database.

21. **Trade Agreements Act of 1979, as Amended**: All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

22. **Ordering Procedures for Federal Supply Schedule Contracts**: Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.
   a. **FAR 8.405-1** Ordering procedures for supplies, and services not requiring a statement of work.
   b. **FAR 8.405-2** Ordering procedures for services requiring a statement of work.

23. **Federal Information Technology Telecommunications Standards Requirements**: Ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.

24. **Federal Information Processing Standards Publications (FIPS PUBS)**: Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the
National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

25. Federal Telecommunication Standards (FED-STDS): Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Acquisition Service, Specification Section, 470 East L’Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202) 619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301) 975-2833.

26. Contractor Tasks/Special Requirements (C-FSS-370) (NOV 2003):

a. Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

b. Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub.L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.

c. Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

d. Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

e. Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

f. Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor’s participation in such order may be restricted in accordance with FAR Part 9.5.
g. Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency’s order.

h. Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency’s order.

i. Government-Furnished Property: As specified by the agency’s order, the Government may provide property, equipment, materials or resources as necessary.

j. Availability of Funds: Many Government agencies’ operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government’s obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

k. Overtime: For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

27. **Contract Administration for Ordering Activities:** Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the ordering activity’s convenience, and (m) Termination for Cause (See 52.212-4)

28. **GSA Advantage!:** GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors’ schedule prices with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

a. Manufacturer;
b. Manufacturer’s Part Number; and
c. Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (ex.: NetScape). The Internet address is [http://www.gsaadvantage.gov](http://www.gsaadvantage.gov)

29. **Purchase of Open Market Items: Note:** Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. ODCs (Other Direct Costs) are not part of this contract and should be treated as open market purchases. Ordering Activities procuring open market items must follow FAR 8.402(f). For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, only if-
a. All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));

b. The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

c. The items are clearly labeled on the order as items not on the Federal Supply Schedule; and

d. All clauses applicable to items not on the Federal Supply Schedule are included in the order.

30. Contractor Commitments, Warranties and Representations:

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

   (1) Time of delivery/installation quotations for individual orders;

   (2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/service/software package submitted in response to requirements which result in orders under this schedule contract.

   (3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

31. Overseas Activities: The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

None: Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis and will only be provided to the Contractor’s technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

32. Blanket Purchase Agreements (BPAs): The use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

33. Contractor Team Arrangements: Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor
team member) must report sales and remit the IFF for all products and services provided under its individual contract.

34. **Installation, Deinstallation, Reinstallation:** The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall receive less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132-8 or 132-9.

35. **Prime Contractor Ordering from Federal Supply Schedules:** Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order—

a. A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

b. The following statement:

This order is placed under written authorization from__________dated__________. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

36. **Insurance- Work On A Government Installation (JAN 1997)(FAR 52.228-5):**

a. The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

b. Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government’s interest shall not be effective—

   (1) For such period as the laws of the State in which this contract is to be performed prescribe; or

   (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.
c. The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance and shall make copies available to the Contracting Officer upon request.

37. Software Interoperability: Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item’s interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at http://www.core.gov.

38. Advance Payments: A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract. (31 U.S.C. 3324)

*NOTE: All non-professional labor categories must be incidental to, and used solely to support professional services, and cannot be purchased separately.

1. SCOPE
   a. The prices, terms and conditions stated under Special Item Numbers 54151S and 54151SHCAS Information Technology Professional Services and Highly Adaptive Cybersecurity 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. For labor-hour orders, the

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:

<table>
<thead>
<tr>
<th>54151S – IT PROFESSIONAL SERVICE RATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>LABOR CATEGORIES</td>
</tr>
<tr>
<td>Program Manager - III</td>
</tr>
<tr>
<td>Program Manager - II</td>
</tr>
<tr>
<td>Program Manager - I</td>
</tr>
<tr>
<td>Project Manager</td>
</tr>
<tr>
<td>Subject Matter Expert - III</td>
</tr>
<tr>
<td>Subject Matter Expert - II</td>
</tr>
<tr>
<td>Database Manager</td>
</tr>
<tr>
<td>Database Management Specialist</td>
</tr>
<tr>
<td>Network Installation Technician</td>
</tr>
<tr>
<td>Help Desk Manager</td>
</tr>
<tr>
<td>Help Desk Specialist</td>
</tr>
<tr>
<td>Training Specialist - III</td>
</tr>
<tr>
<td>Training Specialist - II</td>
</tr>
<tr>
<td>Documentation Specialist</td>
</tr>
<tr>
<td>Research Analyst</td>
</tr>
<tr>
<td>Technical Writer</td>
</tr>
<tr>
<td>Network Security Specialist - III</td>
</tr>
<tr>
<td>Network Security Specialist - II</td>
</tr>
<tr>
<td>Information Assurance Analyst - III</td>
</tr>
<tr>
<td>Information Assurance Analyst - II</td>
</tr>
<tr>
<td>System Design and Development Engineer</td>
</tr>
<tr>
<td>Master Scheduler - II</td>
</tr>
</tbody>
</table>

<p>| 54151HACS – HIGHLY ADAPTIVE CYBERSECURITY SERVICES |
| LABOR CATEGORIES                                |
| Vulnerability Assessment Analyst and Penetration Tester - IV | $242.59 |
| Vulnerability Assessment Analyst and Penetration Tester - III | $206.04 |
| Vulnerability Assessment Analyst and Penetration Tester - II  | $156.95 |</p>
<table>
<thead>
<tr>
<th>Position</th>
<th>Level</th>
<th>Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Assessment Analyst and Penetration Tester - I</td>
<td></td>
<td>$125.75</td>
</tr>
<tr>
<td>Incident Response Analyst - IV</td>
<td></td>
<td>$242.59</td>
</tr>
<tr>
<td>Incident Response Analyst - III</td>
<td></td>
<td>$189.28</td>
</tr>
<tr>
<td>Incident Response Analyst - II</td>
<td></td>
<td>$148.74</td>
</tr>
<tr>
<td>Incident Response Analyst - I</td>
<td></td>
<td>$101.04</td>
</tr>
<tr>
<td>Security Operations Center (SOC) Analyst - IV</td>
<td></td>
<td>$225.91</td>
</tr>
<tr>
<td>Security Operations Center (SOC) Analyst - III</td>
<td></td>
<td>$187.10</td>
</tr>
<tr>
<td>Security Operations Center (SOC) Analyst - II</td>
<td></td>
<td>$146.50</td>
</tr>
<tr>
<td>Security Operations Center (SOC) Analyst - I</td>
<td></td>
<td>$101.17</td>
</tr>
<tr>
<td>Cyber Hunter - IV</td>
<td></td>
<td>$307.14</td>
</tr>
<tr>
<td>Cyber Hunter - III</td>
<td></td>
<td>$213.74</td>
</tr>
<tr>
<td>Cyber Hunter - II</td>
<td></td>
<td>$178.71</td>
</tr>
<tr>
<td>Cyber Hunter - I</td>
<td></td>
<td>$105.75</td>
</tr>
<tr>
<td>Risk and Vulnerability Threat Analyst - IV</td>
<td></td>
<td>$218.49</td>
</tr>
<tr>
<td>Risk and Vulnerability Threat Analyst - III</td>
<td></td>
<td>$174.28</td>
</tr>
<tr>
<td>Risk and Vulnerability Threat Analyst - II</td>
<td></td>
<td>$130.06</td>
</tr>
<tr>
<td>Risk and Vulnerability Threat Analyst - I</td>
<td></td>
<td>$105.04</td>
</tr>
</tbody>
</table>

**LABOR CATEGORY DESCRIPTIONS**

**Program Manager - III**

**Functional Responsibility:** Performs day to day management of overall contract support operations, involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Demonstrates superior written and oral communications skills. Establishes and alters (as necessary) corporate management structure to direct effective contract support activities. Capable of leading multiple projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems.

**Required Experience:** Minimum of fifteen (16) years of IT experience, including at least 8 years of IT and/or telecommunications system management experience. Advanced degree can substitute for years of experience.

**Required Education:** B.A. or B.S. in relevant field.

**Program Manager - II**

**Functional Responsibility:** Performs day to day management of overall contract support operations, involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Demonstrates superior written and oral communications skills. Establishes and alters (as necessary) corporate management structure to direct effective contract support activities. Capable of leading multiple projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems.
**Required Experience:** Minimum of twelve (12) years of IT experience, including at least 8 years of IT and/or telecommunications system management experience. Advanced degree can substitute for years of experience.

**Required Education:** B.A. or B.S. in relevant field.

**Program Manager - II**

**Functional Responsibility:** Performs day to day management of overall contract support operations, involving multiple projects and groups of personnel at multiple locations. Organizes, directs, and coordinates the planning and production of all contract support activities. Demonstrates superior written and oral communications skills. Establishes and alters (as necessary) corporate management structure to direct effective contract support activities. Capable of leading multiple projects that involve the successful management of teams composed of data processing and other information management professionals who have been involved in analysis, design, integration, testing, documenting, converting, extending, and implementing automated information and/or telecommunication systems.

**Required Experience:** Minimum of twelve (8) years of IT experience, including at least 8 years of IT and/or telecommunications system management experience. Advanced degree can substitute for years of experience.

**Required Education:** B.A. or B.S. in relevant field.

**Project Manager**

**Functional Responsibility:** Performs day-to-day management of assigned delivery order projects that involve teams of data processing and other information system and management professionals who have previously been involved in analyzing, designing, integrating, testing, documenting, converting, extending, and implementing automated information and telecommunications systems. Demonstrates proven skills in those technical areas addressed by the delivery order to be managed. Organizes, directs, and coordinates the planning and production of all activities associated with assigned delivery order projects. Demonstrates excellent written and oral communication skills.

**Required Experience:** Minimum of ten (10) years of IT or telecommunications experience, including at least 5 years of IT software management. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. in relevant field.

**Subject Matter Expert - III**

**Functional Responsibility:** Provides technical, managerial, and administrative direction for problem definition, analysis, requirements development, and implementation for complex to extremely complex systems in the subject matter area.

Makes recommendations and advises organization wide improvements, optimization or maintenance efforts in the following specialties: information systems architecture, networking, telecommunications, automation, communications protocols, risk management/electronic analysis, software lifecycle management, software development methodologies, and modeling and simulation.

**Required Experience:** Minimum fifteen (15) years of experience in the IT field with at least ten (10) years of combined new and related older technical experience in the IT field directly related to the required area of expertise. Advanced degree may substitute for years of experience.
**Required Education:** M.A. or M.S. in relevant field. Years of experience may substitute for advanced degree.

**Subject Matter Expert - II**

**Functional Responsibility:** Shall possess senior level skills for Information technology cyber security operations. This individual will provide thought leadership and will have industry experience. SME 2 will utilize expertise with information technology and cyber security when fulfilling customers specifications. SME 2 shall be knowledgeable handling and tracking security events from start to closure; ability to perform analysis, correlate and investigate events to determine their impact on the Enterprise. SME 2 provides support for computer network exploitation and defense techniques to include deterring, identifying and investigating computer and network intrusions; providing incident response and remediation support; performing computer surveillance/monitoring, identifying vulnerabilities; Provides technical support for continuous monitoring, computer exploitation and reconnaissance; Provides technical support for forensics services to include evidence seizure, computer forensic analysis and data recovery, in support of computer crime investigation. Researches and maintains proficiency in open and closed source computer exploitation tools, attack techniques, procedures and trends. Performs research into emerging threat sources and develops threat profiles.

**Required Experience:** Minimum ten (10) years of experience in the IT field with at least ten (10) years of combined new and related older technical experience in the IT field directly related to the required area of expertise. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. in relevant field. Years of experience may substitute for advanced degree.

**Database Manager**

**Functional Responsibility:** Capable of managing the development of database projects. Plans and budgets staff and date resources. Supports application developers in planning, preparation, load analysis, and backup of recovery data. When necessary, responsible for reallocating resources to maximize benefits. Prepares and delivers presentations on DBMS concepts. Provides daily supervision and direction to support staff. Monitors performance and evaluates areas to improve efficiency.

**Required Experience:** Minimum seven (7) years of experience in the development and maintenance of database systems with at least five (5) years of experience with database management systems, system design and analysis, operating systems software, and internal and data manipulation languages. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.

**Database Management Specialist**

**Functional Responsibility:** Provides highly technical expertise and support in the use of DBMSs. Evaluates and recommends available DBMS products to support validated user requirements. Defines file organization, indexing methods, and security procedures for specific user applications. Develops, implements, and maintains database backup and recovery procedures for the environments and ensures that data integrity, security, and recoverability are built into the DBMS applications.

**Required Experience:** Minimum six (6) years of experience in DBMS analysis and programming with at least three (3) years specialized experience in using current DBMS technologies and application design using various database management systems. Advanced degree may substitute for years of experience.
**Required Education:** B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.

**Network Installation Technician**

**Functional Responsibility:** Organizes and directs network installation on site surveys. Assesses and documents current site network configurations. Directs and leads preparation of engineering plans and site installation technical design packages. Develops installation schedules. Mobilizes network installation team. Directs and leads preparation of drawings documenting configuration changes at each site. Prepares site installation test reports. Coordinates post-installation operations and maintenance support.

**Required Experience:** Minimum of eight (8) years of experience with at least five (5) specialized experience including supervision of installation technicians, analysis, design and installation of local and wide area networks and analysis and installation of communications skills. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.

**Help Desk Manager**

**Functional Responsibility:** Provides daily supervision and direction to support staff who are responsible for telephone and in-person support to users in the areas of e-mail, directories, standard Windows desktop applications, and other network services. Manages personnel who serve as the first point of contact for troubleshooting hardware and software PC and printer problems. Excellent written and oral communications skills required.

**Required Experience:** Minimum seven (7) years of experience with at least five (5) years specialized experience including management of help desks in a multi-server environment; comprehensive knowledge of PC operating systems (e.g. DOS, Windows), networking, and mail standards; and supervision of help desk employees. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.

**Help Desk Specialist**

**Functional Responsibility:** Provides telephone and in-person support to users in the areas of email, directories, standard Windows desktop applications, and applications developed under this contract or predecessors. Serves as the initial point of contact for troubleshooting network and hardware and software PC and printer problems.

**Required Experience:** At least five (5) years of experience with a minimum three (3) years of specialized experience including knowledge of PC operating systems (e.g. DOS, Windows) networking and mail standards, and work on a help desk. Advanced degree may substitute for years of experience.

**Required Education:** B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.
Training Specialist - II

Functional Responsibility: Conducts research necessary to develop and revise training courses and prepares appropriate training catalogs. Prepares all instructor materials (course outline, background materials, and training aids). Prepares all student materials (course manuals, workbooks, handouts, completion certificates, and course critique forms). Trains personnel by conducting formal classroom courses, workshops, and seminars. Provides daily supervision of and direction to staff.

Required Experience: Minimum of six (6) years of experience in information system development, training or related fields with at least three (3) years of experience in developing and providing IT and end user training on computer hardware and application software. Advanced degree may substitute for years of experience.

Required Education: B.A. or B.S. degree in relevant field. Years of experience may substitute for advanced degree.

Training Specialist - I

Functional Responsibility: Conducts research necessary to develop and revise training courses and prepares appropriate training catalogs. Prepares all instructor materials (course outline, background material, and training aids). Prepares student materials (course manuals, workbooks handouts, completion certificates, and course critique forms). Trains personnel by conducting formal classroom courses, workshops, seminars. This labor category is offered only in conjunction with IT Professional labor categories.

Required Experience: At least two (2) years of experience in developing and providing IT and end user training on computer hardware and application software. Advanced degree may be substituted for years of experience.

Required Education: Associates Degree in related field. Years of experience may substitute for advanced degree.

Documentation Specialist

Functional Responsibility: Gathers, analyzes, and composes technical information. Conducts research and ensures the use of proper technical terminology. Translates technical information into clear, readable documents to be used by technical and nontechnical personnel. For applications built to run in a Windows environment, uses the standard help compiler to prepare all online documentation.

Required Experience: Minimum of two (2) years’ experience in preparing technical documentation, including conducting research on applicable standards.

Required Education: Associates degree in related field.

Research Analyst

Functional Responsibility: Analyzes existing and potential product and service information and prospective customers and markets. Collates information into meaningful reports and presentation material. Maintains any technical information in a systems library. Performs work through word processing, using electronic spreadsheets and other administrative software products.
**Technical Writer**

**Required Experience:** Minimum of one year of work experience in a business environment. General knowledge of government documents.

**Required Education:** High School Diploma.

**Functional Responsibility:** Assists in collecting and organizing information for preparation of user manuals, training materials, installation guides, proposals, and reports. Edits functional descriptions, system specifications, user manuals, special reports, and any other customer deliverables and documents. Assists in performing financial and administrative functions. Demonstrates the ability to work independently or under only general direction.

**Required Experience:** Minimum of five (5) years of technical writing experience. Advanced degree may be substituted for years of experience.

**Required Education:** Associates degree in related field. Years of experience may substitute for advanced degree.

**Network Security Specialist - III**

**Functional Experience:** Analyzes and defines security requirements for local and wide area networks. Designs, develops, engineers, and implements solutions that meet network security requirements. Responsible for integration and implementation of the network security solution. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development lifecycle.

**Required Experience:** Minimum of eight (8) years of experience, five (5) of which is defining network security requirements for local and wide area networks, evaluation of approved network security product capabilities, configuring standard communications protocols, detecting and analyzing network vulnerabilities, and developing proper computer system security solutions. Advanced degree may be substituted for years of experience.

**Required Education:** B.A. or B.S. degree in related field. Years of experience may substitute for advanced degree.

**Network Security Specialist - II**

**Functional Experience:** Analyzes and defines security requirements for local and wide area networks. Designs, develops, engineers and implements solutions that meet network security requirements. Responsible for integration and implementation of the network security solution. Performs vulnerability and risk analyses of computer systems and applications during all phases of the system development lifecycle.

**Required Experience:** Minimum of four (4) years of experience, two of which is specialized in defining network security requirements for local and wide area networks, evaluating approved network security requirements, configuring standard communication protocols, detecting and analyzing network vulnerabilities and developing proper computer system security solutions. Advanced degree may be substituted for years of experience.

**Required Education:** B.A. or B.S. in relevant field. Years of experience may substitute for advanced degree.
**Information Assurance Specialist - III**

**Functional Experience:** Services performed include, but are not limited to, designing, developing, engineering, and implementing integrated security system solutions that will ensure proprietary/confidential data and systems are protected. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in computer security in the strategic design process to translate security and business requirements into technical designs. Configures and validates secure systems; tests security products and systems to detect security weakness. Conducts regular audits to ensure that systems are being operated securely, and computer security policies and procedures are being implemented as defined in security plans. Duties include architecture design, system/network analysis, vulnerability and risk assessments, and security assessment of hardware and software. Performs duties on tasks that require expertise in firewall, cyber, cloud computing, implementation/configuration, physical security analysis of facilities, security assessment/risk analysis, security design of local area networks and wide area networks, security analysis of network operating systems and applications, continuity of operations, planning, policy development and disaster recovery.

**Required Experience:** Must have a minimum of 7 years of experience. At least 5 years of specialized experience in information assurance and demonstrated ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** B.A. or B.S. degree.

---

**Information Assurance Specialist - III**

**Functional Experience:** Services performed include, but are not limited to, designing, developing, engineering, and implementing integrated security system solutions that will ensure proprietary/confidential data and systems are protected. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs in computer security in the strategic design process to translate security and business requirements into technical designs. Configures and validates secure systems; tests security products and systems to detect security weakness. Conducts regular audits to ensure that systems are being operated securely, and computer security policies and procedures are being implemented as defined in security plans. Duties include architecture design, system/network analysis, vulnerability and risk assessments, and security assessment of hardware and software. Performs duties on tasks that require expertise in firewall, cyber, cloud computing, implementation/configuration, physical security analysis of facilities, security assessment/risk analysis, security design of local area networks and wide area networks, security analysis of network operating systems and applications, continuity of operations, planning, policy development and disaster recovery.

**Required Experience:** Must have a minimum of 4 years of experience. At least 3 years of specialized experience in information assurance and demonstrated ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** B.A. or B.S. degree

---

**System Design and Development Engineer**
**Functional Experience:** Services performed include, but are not limited to, contributing to overall strategic vision and integrates a broad range of solutions in support of client requirements for IT projects. Formulates and defines system scope and objectives, develops or modifies processes to solve complex problems for computer systems and business and electronic interfaces to achieve desired results through the use of innovative technologies. Develops and applies advanced engineering and design methods, theories, and research techniques in the investigation and solution of complex and advanced system requirements, hardware/software interfaces and applications, and solutions. Responsible for design, development, engineering, integration, and architecture. Senior staff manages, plans, and conducts major phases of significant projects. In general, work complexity and responsibility will be greater at higher levels.

**Required Experience:** At least 5 years of specialized experience in system design.

**Required Education:** B.A. or B.S. degree

**Master Scheduler - II**

**Functional Experience:** Responsible for planning, scheduling, coordinating, and monitoring systems/products through the complete system life cycle. Utilizing Gantt, PERT, milestone charts, earned value management and other project management techniques to gauge progress and performance variances to facilitate focus and intervention in critical areas, managing scheduling statement of work (SOW) working with associated project controllers to ensure schedule and budget/forecast are consistent, analyzing schedule for critical path, recognizing implications of changes and assisting in the development and incorporation of work-around plans into the schedule when change is required. Developing necessary reports and metrics to enable management decisions, Utilizing the Earned Value Management (EVM) system to analyze schedules to ensure they are consistent with budgets and forecast and providing integrated scheduling from proposal through execution phase of contract.

**Required Experience:** Must have a minimum of 8 years of experience. At least 2 years of experience in information technology.

**Required Education:** B.A. or B.S. degree.

**Vulnerability Assessment Analyst and Penetration Tester - IV**

**Functional Experience:** May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: Devising and/or selecting appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; listing all steps involved for executing selected test(s) and coaching others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies. Coordinating or leading teams to conduct ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness. Conducting reconnaissance, target assessment, target selection, and vulnerability research. Creating custom tools and exploits to penetrate various levels of controls including network, operating system, and physical. Using COTS or custom tools, conducting or leading teams to conduct vulnerability assessments, analyzing results, identifying exploitable vulnerabilities, and verifying vulnerabilities through manual assessment. Preparing and reviewing assessment documents, validating and communicating key findings to stakeholders.

**Required Experience:** Must have a minimum of 6 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree
Vulnerability Assessment Analyst and Penetration Tester - III

**Functional Experience:** May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: Contributing to the selection of appropriate technical tests, network or vulnerability scan tools, and/or pen testing tools based on review of requirements and purpose; listing all steps involved for executing selected test(s) and coaching others in the use of advanced research, development, or scan tools and the analysis of comparative findings between proposed and current technologies. Coordinating or leading teams to conduct ethical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness. Conducting reconnaissance, target assessment, target selection, and vulnerability research. Using COTS tools, conducting or leading teams to conduct vulnerability assessments, analyzing results, identifying exploitable vulnerabilities, and verifying vulnerabilities through manual assessment. Preparing and reviewing assessment documents, validating and communicating key findings to stakeholders.

**Required Experience:** Must have a minimum of 5 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

---

Vulnerability Assessment Analyst and Penetration Tester - II

**Functional Experience:** May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: Supporting development of and following general test and evaluation plans to compare current and proposed technologies; assessing test results to determine whether they match requirements specifications. Assisting in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness. Conducting reconnaissance, target assessment, data gathering, and vulnerability research. Leveraging COTS tools to conduct vulnerability assessments, analyzing results, identifying exploitable vulnerabilities, and verifying vulnerabilities. Preparing report documents by tailoring technical information and creating benchmark or security authorization reports; outlining key findings related to speed, risks, results and reliability, and recommending acceptance or rejection of technology for applied use.

**Required Experience:** Must have a minimum of 3 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

---

Vulnerability Assessment Analyst and Penetration Tester - I

**Functional Experience:** May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Duties may include: Executing tests by following the steps and procedures listed in a test plan and documenting results in a standardized format that is appropriate for future analyses. Assisting in the coordination of technical tests, network scans, and/or vulnerability scans that support the evaluation of information safeguard effectiveness. Conducting reconnaissance data gathering and vulnerability research. Assisting in the creation of risk and vulnerability reporting.

**Required Experience:** Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree
Risk and Vulnerability Threat Analyst - IV

Functional Experience: Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: Being able to actively lead and manage project update briefings, working sessions, and stakeholder meetings. Applying strong analytical/assessment to security systems and enterprise architecture (e.g., conducting gap analyses, risk assessments.) Participating in Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough reports of the risks to the system and its data. Evaluating system findings, developing PO&AMs, and briefing stakeholders on key findings, recommendations, risk, and impact.

Required Experience: Must have a minimum of 10 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

Required Education: Bachelor’s degree

Risk and Vulnerability Threat Analyst - III

Functional Experience: Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: Supporting engineering design teams by assessing network and system security design features and making recommendations concerning overall security accreditation readiness and compliance and best practices. Supporting interoperability assessment teams and presenting written analyses and conclusions in all phases of analysis. Developing and analyzing system and security documentation. Following up with site administrators for status on non-compliant platforms and maintaining any necessary exception documentation. Maintaining documentation for exceptions to standards. Participating in Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough reports of the risks to the system and its data. Evaluating system findings, developing PO&AMs, and briefing stakeholders on key findings, recommendations, risk, and impact.

Required Experience: Must have a minimum of 7 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

Required Education: Bachelor’s degree

Risk and Vulnerability Threat Analyst - II

Functional Experience: Participates in the conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: Developing, documenting, and executing containment strategies. Documenting and briefing the business on remediation options and executing the plan with stakeholders. Producing final reports and recommendations. Coordinating efforts of—and providing timely updates to—multiple business units during response. Performing in-depth analysis in support of incident response operations. Developing requirements for technical capabilities for cyber incident management. Investigating major breaches of security and recommending appropriate control improvements. Working with infrastructure and application support teams to drive closure of follow up actions identified through incident and problem management. Performing Security Control Assessments on systems to validate the results of risk assessments and ensure that controls in the security plan are present and operating correctly on the system; providing thorough reports of the risks to the system and its data. Evaluating system findings, developing PO&AMs, and briefing stakeholders on key findings, recommendations, risk, and impact.

Required Experience: Must have a minimum of 5 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

Required Education: Bachelor’s degree
Risk and Vulnerability Threat Analyst - I

**Functional Experience:** Participates in conduct of controls and security assessments to assess risk of exposure of proprietary data through weaknesses in platforms, access procedures, or forms of access to the organization’s systems and the data contained in them. Duties may include: Providing technical support on post-event network security logs and trend analysis. Uncovering security and compliance violations. Associating and correlating IP address-related events with specific systems or devices in the IT infrastructure. Supporting development and analysis of system and security documentation. Maintaining documentation for exceptions to standards.

**Required Experience:** Must have a minimum of 4 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

Cyber Hunter - IV

**Functional Experience:** May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization’s data and access to its technology and communications systems. Duties may include: Leading Cyber Hunt team, providing oversight, and bearing responsibility for event investigation and tracking activities. Identifying, deterring, monitoring, and investigating computer and network intrusions. Providing computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery. Monitoring and assessing complex security devices for patterns and anomalies from raw events (DNS, DHCP, AD, SE logs); tagging events for Tier 1 and 2 monitoring. Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware.

**Required Experience:** Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

Cyber Hunter - III

**Functional Experience:** May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization’s data and access to its technology and communications systems. Duties may include: Identifying, deterring, monitoring, and investigating computer and network intrusions. Providing computer forensic support to high technology investigations in the form of evidence seizure, computer
forensic analysis, and data recovery. Monitoring and assessing complex security devices for patterns and anomalies from raw events (DNS, DHCP, AD, SE logs); tagging events for Tier 1 and 2 monitoring. Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware.

**Required Experience:** Must have a minimum of 7 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Cyber Hunter - II**

**Functional Experience:** May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization’s data and access to its technology and communications systems. Duties may include: Using current hashing algorithms to validate forensic images; diagramming networks and imaging servers to support digital forensics operations. Utilizing a variety of industry-standard tools and techniques to collect a system’s current-state data and catalog, document, extract, collect, and preserve information. Using dynamic analysis to identify network intrusions and network monitoring tools to capture real-time traffic spawned by any running malicious code; identifying internet activity that is triggered by malware; identifying network/host-based characteristics and assisting in drafting recommendations to detect and prevent malware infections in the future. Monitoring and assessing complex security devices for patterns and anomalies (IDS, DLP); tagging events for Tier 1 monitoring. Pinpointing location of compromised systems and devices; correlating events from the various components in the IT security infrastructure and identifying attacks and breaches.

**Required Experience:** Must have a minimum of 4 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Cyber Hunter - I**

**Functional Experience:** May respond to crises or urgent situations to mitigate immediate and potential threats. Approaches may include the use of information and threat intelligence specifically focused on a proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities. May identify and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; designs and administers procedures in the organization that sustain the security of the organization’s data and access to its technology and communications systems. Duties may include: Utilizing various government and commercial resources to research known malware and attacks, define their characteristics, and report findings and mitigation recommendations to appropriate personnel. Using prescribed methods and materials to review and analyze events indicative of incidents. Attempting to detect the full spectrum of known cyber-attacks (e.g., DDoS, malware, phishing.) Pinpointing location of compromised systems and devices; correlating events from the various components in the IT security infrastructure and identifying attacks and breaches.

**Required Experience:** Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree
**Incident Response Analyst - IV**

**Functional Experience:** Contributes to generating responses to crises or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: Leading one or more functional security teams (incident response, forensics, cyber intelligence etc.) Supporting the development of staff schedules and staffing forecasts for approval. Ensuring that shift members follow the appropriate incident escalation and reporting procedures. Providing support promptly and efficiently through front-line telephone and email communications. Ingesting, triaging, prioritizing, assigning, tracking, documenting, and managing incidents and results. Providing technical support in response to computer security incidents. Correlating, mapping, and fusing any and all incident information for the development and distribution of cyber alerts and notices, or other products as required. Documenting technical details of current or potential intruder threats consistent with environment. Coordinating, communicating, sharing information, and working closely with organizational stakeholders. Bearing responsibility for knowledge management of operational procedures and support documentation.

**Required Experience:** Must have a minimum of 7 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Incident Response Analyst - III**

**Functional Experience:** Contributes to generating responses to crisis or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: Leading shifts and functional IR teams, providing oversight for incident data flow and response, content, and remediation, and partnering with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets. Performing real-time proactive event investigation on various security enforcement systems, such as SIEM, anti-virus, internet content filtering/reporting, malcode prevention, firewalls, IDS & IPS, web security, anti-spam, etc. Performing the role of Incident Coordinator for IT security events requiring focused response, containment, investigation, and remediation. Performing forensic analysis on hosts supporting investigations. Conducting malware analysis in out-of-band environment (static and dynamic), including complex malware. Coordinating response action to identifies threats and incidents. Analyzing operational anomalies and network behavior, performing mitigation cyber threat monitoring and anomaly analysis, and actively monitoring the networks for cybersecurity threats and vulnerabilities. Providing oversight and perform quality assurance on incident closures. Assisting with knowledge management - Standard Operating Procedures (SOP) and procedural support data

**Required Experience:** Must have a minimum of 5 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Incident Response Analyst - II**

**Functional Experience:** Contributes to generating responses to crisis or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: Providing oversight for incident data flow and response, content, and remediation,
and partnering with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and assets. Performing real-time proactive event investigation on various security enforcement systems, such as SIEM, anti-virus, internet content filtering/reporting, malware prevention, firewalls, IDS & IPS, web security, anti-spam, etc. Performing the role of Incident Coordinator for IT security events requiring focused response, containment, investigation, and remediation. Performing forensic analysis on hosts supporting investigations. Conducting malware analysis in out-of-band environment (static and dynamic), including complex malware.

**Required Experience:** Must have a minimum of 2 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Incident Response Analyst - I**

**Functional Experience:** Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Duties may include: Handling and responding to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Receiving incident reporting, conducting ticket updates, and notifying stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalate when necessary as well as coordinating response to computer security incidents. Recommending a course of action on each incident and creating, managing, and recording all actions taken; serving as initial POC for Events of Interest reported both internally and externally. Establishing alarm/incident escalation process and tracking, following up, and resolving incidents. Initiating and maintaining contact with affected parties during incident response lifecycle; investigating potential incidents/intrusions.

**Required Experience:** Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

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

**Functional Experience:** Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks, provides in-depth incident analysis, evaluates security incidents, and provides proactive threat research. Tracks investigation results and reports on findings. Duties may include: Leading multiple functional security teams, providing management and leadership of SOC. Using knowledge of regulatory compliance directives to include various monitoring and reporting requirements and industry best practices; implementing optimal workflows and procedures. Managing and ensuring the timely response and investigations of security events and incidents by the security operations center. Creating and maintaining schedules to ensure coverage by operations support personnel. Coordinating with threat operations and threat intelligence specialists to resolve high or critical severity level incidents. Bearing responsibility for knowledge management and developing procedures and policies for initial stand-up of a SOC.

**Required Experience:** Must have a minimum of 7 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

**Security Operations Center (SOC) Analyst - III**
**Functional Experience:** Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks. Tracks investigation results and reports on findings. Duties may include: Supporting a Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents and providing first-tier response to security incidents. Leading shifts and functional IR teams, providing oversight and bearing responsibility for event investigation and tracking activities. Supporting Tier 2 operations by monitoring alerts during critical and high-volume events. Conducting more in-depth analyses of security incidents to identify incidents of compromise. Performing intrusion scope and root cause analyses and assisting with intrusion remediation, strategy development, and implementation; recommending effective process changes to enhance defense and response procedures. Using SOC monitoring devices to review and analyze pre-defined events indicative of incidents; creating and recommending content to detect security events. Conducting malware analysis in out-of-band environments (static and dynamic), including complex malware. Vetting IOCs and conducting intelligence vetting and disposition, assessing feed viability. Performing network forensics and deep packet analysis. Identifying countermeasures to detect and prevent security incidents. Supporting knowledge management and developing procedures and policies for initial stand-up of a SOC.

**Required Experience:** Must have a minimum of 5 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

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

**Functional Experience:** Provides cyber threat analysis and reporting to support SOC and program situational awareness. Actively monitors security threats and risks. Tracks investigation results and reports on findings. Duties may include: Supporting Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents and providing first-tier response to security incidents. Monitoring network traffic for security events and performing triage analysis to identify security incidents. Responding to computer security incidents by collecting, analyzing, preserving digital evidence, and ensuring that incidents are recorded and tracked in accordance with SOC requirements. Working closely with the other teams to assess risk and provide recommendations for improving security posture. Recommending content to detect security events. Managing cases within incident management systems. Performing network forensics and deep packet analysis. Identifying countermeasures to detect and prevent security incidents.

**Required Experience:** Must have a minimum of 2 years of experience. Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.

**Required Education:** Bachelor’s degree

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

**Functional Experience:** Provides cyber threat analysis and reporting to support SOC and Program situational awareness. Actively monitors security threats and risks, tracks investigation results, and reports on findings. Duties may include: Supporting Security Operations Center, monitoring security tools to review and analyze pre-defined events indicative of incidents and providing first-tier response to security incidents. Following SOPs for detecting, classifying, and reporting incidents under the supervision of Tier 2 and Tier 3 staff. Managing cases within incident management systems.

**Required Experience:** Demonstrate the ability to communicate orally and in writing and a positive customer service attitude.
**Required Education:** Bachelor’s degree

<table>
<thead>
<tr>
<th>Required Experience or Degree or Relevant Certification</th>
<th>Equivalent Experience or Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-year specialized experience</td>
<td>3 years’ general professional experience</td>
</tr>
<tr>
<td>Relevant certification (e.g., CISSP, PMP, CCNA, etc.)</td>
<td>6 months’ specialized experience</td>
</tr>
<tr>
<td>Associate degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill</td>
<td>1.5 years’ specialized experience</td>
</tr>
<tr>
<td>Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill</td>
<td>3 years’ specialized experience</td>
</tr>
<tr>
<td>Master’s degree in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill</td>
<td>5 years’ specialized experience</td>
</tr>
<tr>
<td>Doctorate in Computer Science, Information Systems, Engineering, Business, or a scientific or technical discipline related to the specific skill</td>
<td>7 years’ specialized experience</td>
</tr>
</tbody>
</table>