AUTHORIZED
INFORMATION TECHNOLOGY SCHEDULE PRICELIST
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY

SPECIAL ITEM NUMBER 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES
SPECIAL ITEM NUMBER 54151HACS - HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
SPECIAL ITEM NUMBER OLM - ORDER LEVEL MATERIALS (OLM)

Note 1: All non-professional labor categories must be incidental to and used solely to support hardware, software and/or professional services, and cannot be purchased separately.

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology Schedule is not to be used as a means to procure services which properly fall under the Brooks Act. These services include, but are not limited to, architectural, engineering, mapping, cartographic production, remote sensing, geographic information systems, and related services. FAR 36.6 distinguishes between mapping services of an A/E nature and mapping services which are not connected nor incidental to the traditionally accepted A/E Services.

Note 3: This solicitation is not intended to solicit for the reselling of IT Professional Services, except for the provision of implementation, maintenance, integration, or training services in direct support of a product. Under such circumstances the services must be performance by the publisher or manufacturer or one of their authorized agents.

NetSecurity Corporation
22375 Broderick Drive
Suite 210
Dulles, VA 20166
Phone: (703) 444-9009    Fax: (703) 444-6899
http://www.netsecurity.com

Contract Number:    GS-35F-0288Y
Period Covered by Contract:    March 27, 2012 – March 26, 2022

General Services Administration
Federal Acquisition Service

Pricelist current through Modification # A826, dated March 2021.

Products and ordering information in this Authorized Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! via the Internet at http://www.gsaadvantage.gov.
TABLE OF CONTENTS

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS ................................................................................................................ 1

TERMS AND CONDITIONS APPLICABLE TO ALL SPECIAL ITEM NUMBERS .................. 3

1. SCOPE ............................................................................................................ 3
2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000) .......... 3
3. ORDER ............................................................................................................ 3
4. PERFORMANCE OF SERVICES ...................................................................... 3
5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989) ................................... 4
6. INSPECTION OF SERVICES .......................................................................... 4
7. RESPONSIBILITIES OF THE CONTRACTOR ................................................ 5
8. RESPONSIBILITIES OF THE ORDERING ACTIVITY ................................... 5
9. INDEPENDENT CONTRACTOR .................................................................... 5
10. ORGANIZATIONAL CONFLICTS OF INTEREST ......................................... 5
11. INVOICES ..................................................................................................... 6
12. PAYMENTS ................................................................................................... 6
13. RESUMES ..................................................................................................... 6
14. INCIDENTAL SUPPORT COSTS ..................................................................... 6
15. APPROVAL OF SUBCONTRACTS .............................................................. 6
16. DESCRIPTION OF IT/IAM PROFESSIONAL SERVICES AND PRICING SIN 54151S... 7

Principal Security Engineer ................................................................. 7
Sr. Security Engineer ............................................................................. 7
Security Engineer .................................................................................. 8
Principal Security Consultant ............................................................ 8
Sr. Security Consultant .......................................................................... 9
Security Consultant .............................................................................. 9
Principal Technology Consultant ...................................................... 10
Sr. Technology Consultant ................................................................. 10
Technology Consultant ......................................................................... 10
Project Manager .................................................................................. 11
Lead Computer Forensics Analyst ....................................................... 11
Sr. Computer Forensics Analyst .......................................................... 12
Computer Forensics Analyst ................................................................. 12
E-Discovery Analyst ............................................................................. 13
Subject Matter Expert ........................................................................... 13
Administrative Assistant ......................................................................... 14
Technical Writer ..................................................................................... 14
Information Assurance (IA) Specialist .................................................. 15
LABOR CATEGORIES FOR SIN 54151S .......................................................... 16
1. SCOPE ............................................................................................................ 18
2. ORDER ............................................................................................................ 18
3. PERFORMANCE OF SERVICES ............................................................... 18
4. INSPECTION OF SERVICES ...................................................................... 19
5. RESPONSIBILITIES OF THE CONTRACTOR .......................................................... 19
6. RESPONSIBILITIES OF THE ORDERING ACTIVITY ........................................ 19
7. INDEPENDENT CONTRACTOR ...................................................................... 19
8. ORGANIZATIONAL CONFLICTS OF INTEREST ............................................ 19
9. INVOICES ..................................................................................................... 20
10. RESUMES .................................................................................................... 20
11. APPROVAL OF SUBCONTRACTS ................................................................. 20
12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING
    21

SIN 54151HACS .................................................................................................. 21
Principal Security Engineer .................................................................................. 22
Sr. Security Engineer .......................................................................................... 23
Security Engineer ............................................................................................... 23
Principal Security Consultant ............................................................................. 24
Sr. Security Consultant ....................................................................................... 24
Security Consultant ............................................................................................ 24
Principal Technology Consultant ....................................................................... 25
Sr. Technology Consultant ................................................................................ 25
Technology Consultant ....................................................................................... 26
Project Manager ................................................................................................. 26
Lead Computer Forensics Analyst .................................................................... 27
Sr. Computer Forensics Analyst ........................................................................ 27
Computer Forensics Analyst ............................................................................... 28
E-Discovery Analyst ........................................................................................... 28
Subject Matter Expert ......................................................................................... 29
Administrative Assistant ..................................................................................... 29
Technical Writer ................................................................................................. 29
Information Assurance (IA) Specialist ................................................................. 30
LABOR CATEGORIES FOR SIN 54151HACS ....................................................... 31
INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS

1a. Table of awarded special item number(s) with appropriate cross-reference to item descriptions and awarded price(s). See Price Charts Below

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. See Price Charts Below

1c. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles, experience, functional responsibility and education for those types of employees or subcontractors who will perform services shall be provided. If hourly rates are not applicable, indicate “Not applicable” for this item. See Pricing Charts Below

2. Maximum order. $500,000.00 for SINs 54151S and 54151HACS; $250,000.00 for SIN OLM

3. Minimum order. $100 for all awarded SINs (54151S, 54151HACS, and OLM)

4. Geographic coverage (delivery area). The Geographic Scope of Contract will be domestic delivery only.

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

<table>
<thead>
<tr>
<th>NetSecurity Corporation</th>
</tr>
</thead>
<tbody>
<tr>
<td>22375 Broderick Drive</td>
</tr>
<tr>
<td>Suite 210</td>
</tr>
<tr>
<td>Dulles, VA 20166</td>
</tr>
</tbody>
</table>

6. Discount from list prices or statement of net price. See Pricing Chart Below

7. Quantity discounts. None

8. Prompt payment terms. 1% 15; NET 30 days from receipt of invoice or date of acceptance, whichever is later.

9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold.

9b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold.

10. Foreign items (list items by country of origin). None

11a. Time of delivery. (Contractor insert number of days.)

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Task Order Dependent</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Task Order Dependent</td>
</tr>
<tr>
<td>OLM</td>
<td>Task Order Dependent</td>
</tr>
</tbody>
</table>

11b. Expedited Delivery. Need to contact the contractor.

11c. Overnight and 2-day delivery. Need to contact the contractor.

11d. Urgent Requirements. Need to contact the contractor
12. F.O.B. point(s). Destination

13a. Ordering address(es).

<table>
<thead>
<tr>
<th>Ordering Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetSecurity Corporation</td>
</tr>
<tr>
<td>22375 Broderick Drive</td>
</tr>
<tr>
<td>Suite 210</td>
</tr>
<tr>
<td>Dulles, VA 20166</td>
</tr>
</tbody>
</table>

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

14. Payment address(es).

<table>
<thead>
<tr>
<th>Payment Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetSecurity Corporation</td>
</tr>
<tr>
<td>22375 Broderick Drive</td>
</tr>
<tr>
<td>Suite 210</td>
</tr>
<tr>
<td>Dulles, VA 20166</td>
</tr>
</tbody>
</table>

15. Warranty provision. Standard Warranty

16. Export packing charges, if applicable. N/A

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

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

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

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

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

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

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

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

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

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

25. Data Universal Number System (DUNS) number: 12-2657005

26. Notification regarding registration in Systems for Award Management (SAM). NetSecurity Corporation is registered in SAM. Cage Code: 3CJ4
TERMS AND CONDITIONS APPLICABLE TO ALL SPECIAL ITEM NUMBERS

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

2. PERFORMANCE INCENTIVES 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/IAM Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

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

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

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

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

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

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

6. INSPECTION OF SERVICES

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

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/IAM Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS

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

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

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

       (1) The offeror;

       (2) Subcontractors; and/or

       (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

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

15. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.
16. DESCRIPTION OF IT/IAM PROFESSIONAL SERVICES AND PRICING SIN 54151S

Principal Security Engineer

Functional Responsibility: Provides leadership, technical supervision, and mentorship to security engineers. Must have experience in 7 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DITSCAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

Minimum/General Experience: 8 years of work experience. Task leadership experience. CISM, CISA, GSEC, CISSP, or equivalent information security certification desirable.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field. Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Security Engineer

Functional Responsibility: Ability to work independently with minimal technical oversight. Must have experience in 5 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DITSCAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing

Minimum/General Experience: 5 years of work experience.
Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Security Engineer

**Functional Responsibility:** Typically works under technical supervision and mentorship of senior security engineers. Must have experience in 3 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DITSCAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

**Minimum/General Experience:** 2 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Principal Security Consultant

**Functional Responsibility:** Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. May be called upon to manage projects and staff, and mentor less experienced staff. Ability to successfully interface with clients (internal and external), be able to document and explain technical details in a concise, understandable manner; provide training and perform public speaking and be comfortable in front of an audience; and manage team projects.

**Minimum/General Experience:** 8 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.
Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Security Consultant

Functional Responsibility: Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. May be called upon to manage projects and staff, and mentor less experienced staff. Ability to successfully interface with clients (internal and external) and the ability to document and explain technical details in a concise, understandable manner.

Minimum/General Experience: 5 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Security Consultant

Functional Responsibility: Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. Ability to successfully interface with clients (internal and external) and the ability to document and explain technical details in a concise, understandable manner.

Minimum/General Experience: 3 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.
Principal Technology Consultant

Functional Responsibility: Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. When required, researches options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Works closely with design team leader to develop project design. Contributes to design deliverables, serves as consultant for other team members, and certifies that the design is technically sound. Assists team members, allocates work, and helps prepare estimates and schedules. Prepares status reports and reviews and certifies team members' work. Develops or assists in developing project design. Coordinates work groups. Ensures that standards for the project are implemented and that support is available to the end user. Determines training requirements and implements as necessary.

Minimum/General Experience: 8 years of technical experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Technology Consultant

Functional Responsibility: Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. Assists with researching options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Contributes to design deliverables and certifies that the design is technically sound. Assists team members, allocates work, and helps prepare estimates and schedules. Assists in developing project design. Ensures that standards for the project are implemented and that support is available to the end user.

Minimum/General Experience: 5 years of technical experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Technology Consultant

Functional Responsibility: Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. Assists with researching options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Contributes to design deliverables and certifies that the design is technically sound.
sound. Assists team members, allocates work, and helps prepare estimates and schedules. Assists in developing project design. Ensures that standards for the project are implemented and that support is available to the end user.

Minimum/General Experience: 3 years of technical experience.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Project Manager**

**Functional Responsibility:** Responsible for the performance of projects or a definable portion of a larger program in accordance with contract requirements and company policies, procedures and guidelines. Directs and supervises all support resources for the performance of project assignments and activities. Consults with the client staff concerning overall scheduling, work assignments, staffing, progress reporting, security, etc. Responsible for overall quality assurance and timeliness of delivery for all work performed. Also responsible for acquiring follow-on business associated with assigned projects and for supporting new business development.

Minimum/General Experience: 6 years of related experience, including one year in project management.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Lead Computer Forensics Analyst**

**Functional Responsibility:** Provides leadership, technical supervision, and mentorship to forensics analysts. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstands legal scrutiny of opposing counsels. Provides technical guidance and assistance to legal staff while preventing of spoliation of evidence.

Minimum/General Experience: 6 years of work experience in Information Assurance, Information Security, or Forensics technical guidance and leadership. EnCE, CISSP, CHFI, or equivalent certification.
Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Computer Forensics Analyst

Functional Responsibility: Ability to work independently with minimal technical oversight. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensic analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel. Provides technical guidance and assistance to legal staff.

Minimum/General Experience: 4 years of experience in Information Assurance, Security, or Forensics. EnCE, CISSP, CHFI, or equivalent certification.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Computer Forensics Analyst

Functional Responsibility: Typically works under technical supervision and mentorship of senior forensics analyst. Organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensic analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically
sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel.

Minimum Experience: 2 years of experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

E-Discovery Analyst

Functional Responsibility: Responsible for managing electronic discovery data in the processing, analysis, review and production phases of e-discovery including quality control. This position also serves as the expert on various processing and review technologies and acts as a consultant on data conversion issues, search technologies and problem solving. Will consult on data conversion issues, search technologies and problem solving, process e- discovery received from clients for analysis and review, analyze e-discovery and recommend culling strategies prior to review, research and identify technology solutions to resolve e-discovery issues, use critical thinking and trouble-shooting abilities to manage electronic discovery in a defensible manner, Develop new technologies and scripts to increase productivity, educate legal teams and clients on e-discovery issues, systems and processes, monitor and update processing specifications as needed, and test and evaluate new technologies and upgrades. Must have extensive knowledge of the concepts, principles, management and processing of electronically stored information (ESI) including the use of various ESI management and review tools and applications and an in-depth knowledge of search including the ability to demonstrate proficiency with the proper handling of metadata, text extraction, indexing of data.

Minimum Experience: 2 years of experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Subject Matter Expert

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

Minimum Experience: 10 years of experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Administrative Assistant

Functional Responsibility: Provides administrative and secretarial support such as technical typing, editing of word processing and other computer-based manuscripts, integration of various sources into a cohesive product which may be delivered as computer-based magnetic media, preparation of graphical and narrative presentation material. Provides assistance with maintaining personnel and other files; prepares correspondence, schedules and coordinates travel. Supports the development of contract deliverables and reports by developing and updating graphic presentations to improve the quality and enhance the usability of these documents. Responsible for integrating the graphics generated with automated tools and the deliverable documents.

Minimum Experience: 1 year of work experience.

Education: High School Diploma or equivalent.

Technical Writer

Functional Responsibility: Researches, writes, edits, and proofreads technical data for use in documents or sections of documents such as manuals, procedures and specifications. Ensures technical documentation is accurate, complete, meets editorial and government specifications and adheres to standards for quality, graphics, coverage, format, and style. Assists in establishing style guidelines and standards for texts and illustrations or equivalent.

Minimum Experience: 3 years of work related experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, English, business/finance, or related field.

Education and experience requirements may be substituted with:
1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Information Assurance (IA) Specialist

Functional Responsibility: Provides guidance for Information Assurance (IA), including advice on how to adhere to regulatory requirements, such as Federal Information Security Management Act of 2002 (FISMA). Responsible for interpreting IA requirements using DoD, FISMA, and NIST guidelines. Responsible for policy compliance, internal policy development, and strategic planning. May be responsible for monitoring compliance notices and ensuring that security patches, communication tasking orders and warning orders are known. Performs IA consulting, assessment, documentation and IA compliance program development.

Supports programs to comply with or follow FISMA, OMB A-130, NIST Publications, and DoD requirements and guidelines. Prepares and updates C&A packages, such as System Security Plan (SSP), Information Technology Contingency Plan (ITCP), and Privacy Impact Assessments (PIA). Prepares and conducts Security Test and Evaluation (ST&E) for supported systems. Analyzes results of ST&E to produce Plan of Action and Milestones (POA&M). Prepares quarterly FISMA compliance reports as required.

Minimum Experience: 2 years of work related experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.
LABOR CATEGORIES FOR SIN 54151S

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Security Engineer</td>
<td>$171.28</td>
</tr>
<tr>
<td>Sr. Security Engineer</td>
<td>$147.30</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>$119.90</td>
</tr>
<tr>
<td>Principal Security Consultant</td>
<td>$171.28</td>
</tr>
<tr>
<td>Sr. Security Consultant</td>
<td>$147.30</td>
</tr>
<tr>
<td>Security Consultant</td>
<td>$119.90</td>
</tr>
<tr>
<td>Principal Technology Consultant</td>
<td>$158.69</td>
</tr>
<tr>
<td>Sr. Technology Consultant</td>
<td>$136.47</td>
</tr>
<tr>
<td>Technology Consultant</td>
<td>$111.08</td>
</tr>
<tr>
<td>Project Manager</td>
<td>$171.28</td>
</tr>
<tr>
<td>Computer Forensics Analyst</td>
<td>$138.54</td>
</tr>
<tr>
<td>Sr. Computer Forensics Analyst</td>
<td>$178.34</td>
</tr>
<tr>
<td>Lead Computer Forensics Analyst</td>
<td>$196.47</td>
</tr>
<tr>
<td>Electronic Discovery (e-Discovery) Analyst</td>
<td>$120.91</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$222.67</td>
</tr>
<tr>
<td>Administrative Assistant</td>
<td>$56.68</td>
</tr>
<tr>
<td>Technical Writer</td>
<td>$82.22</td>
</tr>
<tr>
<td>Information Assurance (IA) Specialist</td>
<td>$114.86</td>
</tr>
</tbody>
</table>
TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBER 54151HACS)

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

- Federal Acquisition Regulation (FAR) Part 52.204-21
- OMB Memorandum M-06-19 - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- OMB Memorandum M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- OMB Memorandum M-16-03 - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-16-04 – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

****NOTE: All non-professional labor categories must be incidental to, and used solely to support Highly Adaptive Cybersecurity Services, and cannot be purchased separately.
****NOTE: All labor categories under the Special Item Number 54151S Information Technology Professional Services may remain under SIN 54151S unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.

1. SCOPE

   a. The labor categories, prices, terms and conditions stated under Special Item Numbers High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services (SIN 54151HACS) within the scope of this Information Technology Schedule.
   b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132-33, 132-8), and may be quoted along with services to provide a total solution.
   c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
   d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
   e. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. ORDER

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

   b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

3. PERFORMANCE OF SERVICES

   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor’s travel.

4. INSPECTION OF SERVICES


5. RESPONSIBILITIES OF THE CONTRACTOR

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

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST
a. Definitions.

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

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

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

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

9. INVOICES

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

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.
12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

SIN 54151HACS

Penetration Testing

Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. Tasks include but are not limited to:

- Conducting and/or supporting authorized penetration testing on enterprise network assets.
- Analyzing site/enterprise Computer Network Defense policies and configurations and evaluate compliance with regulations and enterprise directives.
- Assisting with the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems, and processes).

Incident Response

Incident response services help organizations impacted by a Cybersecurity compromise determine the extent of the incident, remove the adversary from their systems, and restore their networks to a more secure state. Tasks include but are not limited to:

- Collect intrusion artifacts (e.g., source code, malware, and Trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise.
- Perform command and control functions in response to incidents.
- Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Cyber Hunt

Cyber hunt activities are responses to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks. Investigates and analyzes all relevant response activities.

Tasks include but are not limited to:

- Collecting intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise.
- Coordinating with and provide expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents.
- Correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

Risk Vulnerability Assessment
Risk and vulnerability assessments conduct assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. Tasks include but are not limited to:

- Network Mapping: Consists of identifying assets on an agreed upon IP address space or network range(s).
- Vulnerability Scanning: Comprehensively identifies IT vulnerabilities associated with agency systems that are potentially exploitable by attackers.
- Phishing Assessment: Includes activities to evaluate the level of awareness of the agency’s workforce with regard to digital form of social engineering that uses authentic looking, but bogus, emails request information from users or direct them to a fake Website that requests information. Phishing assessments can include scanning, testing, or both and can be conducted as a one-time event or as part of a larger campaign to be conducted over several months.
- Wireless Assessment: Includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a customer’s facility.
- Web Application Assessment: Includes scanning, testing or both of outward facing web applications for defects in Web service implementation may lead to exploitable vulnerabilities. Provide report on how to implement Web services securely and that traditional network security tools and techniques are used to limit access to the Web Service to only those networks and systems that should have legitimate access.
- Operating System Security Assessment (OSSA): Assesses the configuration of select host operating systems (OS) against standardized configuration baselines.
- Database Assessment: Assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities.
- Penetration Testing: Conducting and/or supporting authorized Penetration Testing on enterprise network assets.

Principal Security Engineer

Functional Responsibility: Provides leadership, technical supervision, and mentorship to security engineers. Must have experience in 7 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DIACAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

Minimum/General Experience: 8 years of work experience. Task leadership experience. CISM, CISA, GSEC, CISSP, or equivalent information security certification desirable.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or a related field.

Education and experience requirements may be substituted with:
1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Security Engineer

Functional Responsibility: Ability to work independently with minimal technical oversight. Must have experience in 5 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DITSCAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

Minimum/General Experience: 5 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Security Engineer

Functional Responsibility: Typically works under technical supervision and mentorship of senior security engineers. Must have experience in 3 or more of the following skill areas: Cloud Computing Security, Mobile Security, and Web Application Security; FISMA, Certification and Accreditation, DITSCAP, NIST SP 800-37; Information Assurance/Security Policies and Procedures; Vulnerability Assessments; NIST Special Publication 800 Series and FIPS; Vulnerability scanning; Risk assessments; Firewall, Intrusion Detection/Prevention, SIM, Configuration Management solutions implementation, configuration, integration, and management; IT/Security audit; Penetration Testing; Forensic Analyses; Encryption, PKI, SSL, SSO, VPN, Strong Authentication, Hashes; Identity Management, HSPD-12; Systems Engineering, UNIX, Mac OS, and Windows Operating Systems; Database Engineering, Oracle, Sybase, SQL Server; Network Engineering, Routers, Switches, Firewalls, NAT, VPN, TCP/IP, Ports/Protocols/Services; Work breakdown structures/project estimation; Technical writing and editing.

Minimum/General Experience: 2 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

3.

**Principal Security Consultant**

**Functional Responsibility:** Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. May be called upon to manage projects and staff, and mentor less experienced staff. Ability to successfully interface with clients (internal and external), be able to document and explain technical details in a concise, understandable manner; provide training and perform public speaking and be comfortable in front of an audience; and manage team projects.

**Minimum/General Experience:** 8 years of work experience.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Sr. Security Consultant**

**Functional Responsibility:** Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. May be called upon to manage projects and staff, and mentor less experienced staff. Ability to successfully interface with clients (internal and external) and the ability to document and explain technical details in a concise, understandable manner.

**Minimum/General Experience:** 5 years of work experience.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Security Consultant**

**Functional Responsibility:** Provides forensics, security, and auditing consultation/analysis. Conducts regulatory compliance, risk assessment, security testing and audits, web application security, infrastructure security, and other cyber security functions. Ability to successfully interface with clients (internal and external) and the ability to document and explain technical details in a concise, understandable manner.
Minimum/General Experience: 3 years of work experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Principal Technology Consultant

Functional Responsibility: Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. When required, researches options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Works closely with design team leader to develop project design. Contributes to design deliverables, serves as consultant for other team members, and certifies that the design is technically sound. Assists team members, allocates work, and helps prepare estimates and schedules. Prepares status reports and reviews and certifies team members' work. Develops or assists in developing project design. Coordinates work groups. Ensures that standards for the project are implemented and that support is available to the end user. Determines training requirements and implements as necessary.

Minimum/General Experience: 8 years of technical experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Technology Consultant

Functional Responsibility: Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. Assists with researching options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Contributes to design deliverables and certifies that the design is technically sound. Assists team members, allocates work, and helps prepare estimates and schedules. Assists in developing project design. Ensures that standards for the project are implemented and that support is available to the end user.

Minimum/General Experience: 5 years of technical experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.
Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Technology Consultant**

**Functional Responsibility:** Works with the client and team to determine technical requirements to find the best possible solution to fit the client's request. Interacts with the client's on-site technical staff, as needed. Assists with researching options toward resolution of client problem, taking into consideration the client's environment, budget and business requirements. Contributes to design deliverables and certifies that the design is technically sound. Assists team members, allocates work, and helps prepare estimates and schedules. Assists in developing project design. Ensures that standards for the project are implemented and that support is available to the end user.

**Minimum/General Experience:** 3 years of technical experience.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Project Manager**

**Functional Responsibility:** Responsible for the performance of projects or a definable portion of a larger program in accordance with contract requirements and company policies, procedures and guidelines. Directs and supervises all support resources for the performance of project assignments and activities. Consults with the client staff concerning overall scheduling, work assignments, staffing, progress reporting, security, etc. Responsible for overall quality assurance and timeliness of delivery for all work performed. Also responsible for acquiring follow-on business associated with assigned projects and for supporting new business development.

**Minimum/General Experience:** 6 years of related experience, including one year in project management.

**Education:** A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.
Lead Computer Forensics Analyst

Functional Responsibility: Provides leadership, technical supervision, and mentorship to forensics analysts. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel. Provides technical guidance and assistance to legal staff while preventing of spoliation of evidence.

Minimum/General Experience: 6 years of work experience in Information Assurance, Information Security, or Forensics technical guidance and leadership. EnCE, CISSP, CHFI, or equivalent certification.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Sr. Computer Forensics Analyst

Functional Responsibility: Ability to work independently with minimal technical oversight. Plans, organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensics examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel. Provides technical guidance and assistance to legal staff.

Minimum/General Experience: 4 years of experience in Information Assurance, Security, or Forensics. EnCE, CISSP, CHFI, or equivalent certification.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.
Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Computer Forensics Analyst

Functional Responsibility: Typically works under technical supervision and mentorship of senior forensics analyst. Organizes, directs and conducts forensic analysis and intrusion investigations on a variety of electronic media. Documents computer network exploitation and defense techniques. Identifies, deters, monitors, and investigates computer and network intrusions. Manages digital forensic examinations through the entire lifecycle of an investigation. Conducts forensics analysis to support malicious software, cyber security incidents, system intrusion, or other (civil, criminal, or internal) investigations. Acquires, collects, documents, and preserves evidence from various forms of electronic media and equipment. Conducts detailed forensically sound investigation of computer storage media, network servers, live systems, and mobile devices to identify and document relevant findings. Develops high quality oral and written work product and presents complex technical matters clearly and concisely. Produces expert reports that withstand legal scrutiny of opposing counsel.

Minimum Experience: 2 years of experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

E-Discovery Analyst

Functional Responsibility: Responsible for managing electronic discovery data in the processing, analysis, review and production phases of e-discovery including quality control. This position also serves as the expert on various processing and review technologies and acts as a consultant on data conversion issues, search technologies and problem solving. Will consult on data conversion issues, search technologies and problem solving, process e-discovery received from clients for analysis and review, analyze e-discovery and recommend culling strategies prior to review, research and identify technology solutions to resolve e-discovery issues, use critical thinking and trouble-shooting abilities to manage electronic discovery in a defensible manner. Develop new technologies and scripts to increase productivity, educate legal teams and clients on e-discovery issues, systems and processes, monitor and update processing specifications as needed, and test and evaluate new technologies and upgrades. Must have extensive knowledge of the concepts, principles, management and processing of electronically stored information (ESI) including the use of various ESI management and review tools and applications and an in-depth knowledge of search including the ability to demonstrate proficiency with the proper handling of metadata, text extraction, indexing of data.

Minimum Experience: 2 years of experience.
Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Subject Matter Expert**

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

**Minimum Experience:** 10 years of experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, forensics, criminal justice, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

**Administrative Assistant**

**Functional Responsibility:** Provides administrative and secretarial support such as technical typing, editing of word processing and other computer-based manuscripts, integration of various sources into a cohesive product which may be delivered as computer-based magnetic media, preparation of graphical and narrative presentation material. Provides assistance with maintaining personnel and other files; prepares correspondence, schedules and coordinates travel. Supports the development of contract deliverables and reports by developing and updating graphic presentations to improve the quality and enhance the usability of these documents. Responsible for integrating the graphics generated with automated tools and the deliverable documents.

**Minimum Experience:** 1 year of work experience.

**Education:** High School Diploma or equivalent.

**Technical Writer**

**Functional Responsibility:** Researches, writes, edits, and proofreads technical data for use in documents or sections of documents such as manuals, procedures and specifications. Ensures technical documentation is accurate, complete, meets editorial and government specifications and adheres to standards for quality, graphics, coverage, format, and style. Assists in establishing style guidelines and standards for texts and illustrations or equivalent.
Minimum Experience: 3 years of work related experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, English, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.

Information Assurance (IA) Specialist

Functional Responsibility: Provides guidance for Information Assurance (IA), including advice on how to adhere to regulatory requirements, such as Federal Information Security Management Act of 2002 (FISMA). Responsible for interpreting IA requirements using DoD, FISMA, and NIST guidelines. Responsible for policy compliance, internal policy development, and strategic planning. May be responsible for monitoring compliance notices and ensuring that security patches, communication tasking orders and warning orders are known. Performs IA consulting, assessment, documentation and IA compliance program development.

Supports programs to comply with or follow FISMA, OMB A-130, NIST Publications, and DoD requirements and guidelines. Prepares and updates C&A packages, such as System Security Plan (SSP), Information Technology Contingency Plan (ITCP), and Privacy Impact Assessments (PIA). Prepares and conducts Security Test and Evaluation (ST&E) for supported systems. Analyzes results of ST&E to produce Plan of Action and Milestones (POA&M). Prepares quarterly FISMA compliance reports as required.

Minimum Experience: 2 years of work related experience.

Education: A Bachelor’s degree in computer science/systems, information systems/technology, software engineering, management, natural sciences, social sciences, mathematics, business/finance, or related field.

Education and experience requirements may be substituted with:

1. Three years of additional applicable experience may be substituted for Bachelor’s degree.
2. A Master’s degree with two years less of experience may be substituted for Bachelor’s degree.
LABOR CATEGORIES FOR SIN 54151HACS

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>GSA Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principal Security Engineer</td>
<td>$171.28</td>
</tr>
<tr>
<td>Sr. Security Engineer</td>
<td>$147.30</td>
</tr>
<tr>
<td>Security Engineer</td>
<td>$119.90</td>
</tr>
<tr>
<td>Principal Security Consultant</td>
<td>$171.28</td>
</tr>
<tr>
<td>Sr. Security Consultant</td>
<td>$147.30</td>
</tr>
<tr>
<td>Security Consultant</td>
<td>$119.90</td>
</tr>
<tr>
<td>Principal Technology Consultant</td>
<td>$158.69</td>
</tr>
<tr>
<td>Sr. Technology Consultant</td>
<td>$136.47</td>
</tr>
<tr>
<td>Technology Consultant</td>
<td>$111.08</td>
</tr>
<tr>
<td>Project Manager</td>
<td>$171.28</td>
</tr>
<tr>
<td>Computer Forensics Analyst</td>
<td>$138.54</td>
</tr>
<tr>
<td>Sr. Computer Forensics Analyst</td>
<td>$178.34</td>
</tr>
<tr>
<td>Lead Computer Forensics Analyst</td>
<td>$196.47</td>
</tr>
<tr>
<td>Electronic Discovery (e-Discovery) Analyst</td>
<td>$120.91</td>
</tr>
<tr>
<td>Subject Matter Expert</td>
<td>$222.67</td>
</tr>
<tr>
<td>Administrative Assistant</td>
<td>$56.68</td>
</tr>
<tr>
<td>Technical Writer</td>
<td>$82.22</td>
</tr>
<tr>
<td>Information Assurance (IA) Specialist</td>
<td>$114.86</td>
</tr>
</tbody>
</table>