GENERAL SERVICES ADMINISTRATION

Federal Supply Service
Authorized Federal Supply Schedule Price List

Multiple Award Schedule
Code F – Information Technology
F.03 – IT Services Subcategory

Special Item Number 54151S – IT Professional Services
Special Item Number 54151HACS – Highly Adaptive Cyber Security Services
Special Item Number OLM – Order Level Materials

Jacobs Technology Inc.
600 William Northern Blvd.
Tullahoma, TN 37388-4729
www.jacobstechnology.com

Point of Contact for Contract Administration: Darin Williams
Phone: (610) 238-1009
Fax: (931) 393-6210
Email Address: Darin.Williams@jacobs.com

Contract Number: 47QTCA20D001R
Period Covered by Contract: 11/05/2019 – 11/04/2024 (Base Period) plus
Three Additional Option Periods of Five Years Each

Pricelist current through: Modification #PA-0004, dated June 18, 2020

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

For more information on ordering from Federal Supply Schedules click on the FSS Schedules button at fss.gsa.gov.
TABLE OF CONTENTS

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS ........................................... 1
1. GEOGRAPHIC SCOPE OF CONTRACT: .................................................................................. 1
2. CONTRACTOR'S ORDERING ADDRESS AND PAYMENT INFORMATION: ........................................ 1
3. LIABILITY FOR INJURY OR DAMAGE: .................................................................................. 1
4. STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279:........ 2
5. FOB DESTINATION, (CONUS AND OCONUS) ...................................................................... 2
6. DELIVERY SCHEDULE: ...................................................................................................... 2
7. DISCOUNTS: ...................................................................................................................... 2
8. TRADE AGREEMENTS ACT OF 1979, AS AMENDED: ........................................................ 2
9. STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING: .................................... 3
10. SMALL REQUIREMENTS: .................................................................................................. 3
11. MAXIMUM ORDER: ......................................................................................................... 3
12. ORDERING PROCEDURES FOR FEDERAL SUPPLY SCHEDULE CONTRACTS: ............................. 3
13. FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION STANDARDS REQUIREMENTS: ...... 3
13.1. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS): ...................... 3
13.2. FEDERAL TELECOMMUNICATION STANDARDS (FED-STDs): ....................................................... 4
14. CONTRACT OR TASKS/ SPECIAL REQUIREMENTS: ............................................................ 4
15. CONTRACT ADMINISTRATION FOR ORDERING OFFICES: .................................................. 5
16. GSA Advantage! .................................................................................................................. 5
17. PURCHASE OF OPEN MARKET ITEMS ............................................................................. 5
18. CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS ............................. 5
19. OVERSEAS ACTIVITIES .................................................................................................... 6
20. BLANKET PURCHASE AGREEMENTS (BPAs) ..................................................................... 6
21. CONTRACTOR TEAM ARRANGEMENTS ............................................................................ 6
22. INSTALLATION, DE-INSTALLATION, REINSTALLATION ............................................................. 6
23. SECTION 508 COMPLIANCE ............................................................................................... 6
24. INSURANCE—WORK ON A GOVERNMENT INSTALLATION (JAN 1997) (FAR 52.228-5) 28.310 .... 7
25. SOFTWARE INTEROPERABILITY ........................................................................................ 7
26. ADVANCE PAYMENTS ....................................................................................................... 7
27. ORDER-LEVEL MATERIALS .............................................................................................. 7

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

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS) (SPECIAL ITEM NUMBERS 54151HACS) ...................................................... 13
1. SCOPE ............................................................................................................................... 13
2. ORDER .............................................................................................................................. 15
3. PERFORMANCE OF SERVICES ....................................................................................... 15
4. INSPECTION OF SERVICES ............................................................................................. 15
5. RESPONSIBILITIES OF THE CONTRACTOR .................................................................... 15
6. RESPONSIBILITIES OF THE ORDERING ACTIVITY ......................................................... 16
7. INDEPENDENT CONTRACTOR................................................................. 16
8. ORGANIZATIONAL CONFLICTS OF INTEREST.................................... 16
9. INVOICES ........................................................................................ 16
10. RESUMES ..................................................................................... 16
11. APPROVAL OF SUBCONTRACTS .................................................... 16
12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING ............................................................................................................................. 16
   SIN 54151S – GOVERNMENT SITE IT PROFESSIONAL SERVICES LABOR RATES ................................................................. 18
   SIN 54151S – CONTRACTOR SITE IT PROFESSIONAL SERVICES LABOR RATES ................................................................................................................................. 18
   SIN 54151HACS – GOVERNMENT SITE HACS LABOR RATES ................................................................................................................................. 20
   SIN 54151HACS – CONTRACTOR SITE HACS LABOR RATES ................................................................................................................................. 21
LABOR CATEGORY QUALIFICATION EQUIVALENCIES ................................................................. 22
   SIN 54151S IT PROFESSIONAL SERVICES LABOR CATEGORY DESCRIPTIONS ................................................................. 23
   1. Administrative Support ... ........................................................................ 23
   2. Analyst ................................................................................................... 23
   3. Business Analyst I .............................................................................. 23
   4. Business Analyst II ............................................................................ 23
   5. Consultant I .......................................................................................... 24
   6. Consultant II ...................................................................................... 24
   7. Consultant III ..................................................................................... 24
   8. Help Desk Operator ............................................................................ 24
   9. Information Engineer .......................................................................... 25
  10. Network Engineer ................................................................................ 25
  11. Network Operating Center Technician .................................................. 25
  12. Principal / Partner ............................................................................ 25
  13. Program Manager ............................................................................... 25
  14. Programmer/Analyst III ................................................................... 26
  15. Programmer/Analyst I ..................................................................... 26
  16. Programmer/Analyst II ................................................................... 26
  17. Project Manager ............................................................................... 27
  18. Quality Assurance (QA) / Test Engineer .............................................. 27
  19. Security Engineer ............................................................................ 27
  20. Senior System Architect .................................................................... 27
  21. Software Architect .......................................................................... 28
  22. System Administrator ....................................................................... 28
  23. Systems Engineer ............................................................................ 28
  24. Technical Writer .............................................................................. 28
  25. Telecom Engineer I .......................................................................... 29
  26. Telecom Engineer II ........................................................................ 29
  27. Telecom Engineer III ....................................................................... 29
  28. Information Assurance Engineer I ....................................................... 29
  29. Information Assurance Engineer II ..................................................... 30
  30. Information Assurance Engineer III ................................................... 30
  31. Information Assurance Policy Analyst ................................................ 30
  32. Senior Information Assurance Policy Analyst ..................................... 31
  33. Information Assurance Subject Matter Expert ................................. 31
  34. Senior System Administrator ............................................................ 31
  35. Program Control Specialist ............................................................... 32
  36. Senior Administrative Support ......................................................... 32

SIN 54151HACS HIGHLY ADAPTIVE CYBERSECURITY LABOR DESCRIPTIONS ................................................................. 33
   1. Penetration Testing Team - Principal ................................................ 33
   2. Penetration Testing Team - Subject Matter Expert (SME) .................. 33
   3. Penetration Testing - Analyst I .......................................................... 33
   4. Penetration Testing - Analyst II ....................................................... 34
   5. Penetration Testing - Analyst III ....................................................... 34
   6. Penetration Testing - Analyst IV ....................................................... 35
   7. Penetration Testing - Manager/Lead ................................................ 35
   8. Incident Response Team - Principal ................................................. 35
   9. Incident Response Team - Subject Matter Expert (SME) ................ 36
  10. Incident Detection/Response Analyst II ............................................ 36

Jacobs Technology Inc.
Contract Number 47QTCA20D001R
Page ii
11. Incident Detection/Response Analyst III ................................................................. 36
12. Incident Detection/Response Analyst IV ................................................................. 37
13. Incident Detection/Response Manager - Lead ......................................................... 37
14. Security Operations Center (SOC) Analyst I ......................................................... 37
15. Security Operations Center (SOC) Analyst II ....................................................... 37
16. Security Operations Center (SOC) Analyst III ..................................................... 38
17. Security Operations Center (SOC) Analyst IV ..................................................... 38
18. Security Operations Center (SOC) – Manager/Lead ............................................. 38
19. Cyber Hunt Team - Principal .................................................................................. 39
20. Cyber Hunt Team - Subject Matter Expert (SME) ................................................. 39
21. Malware Detection Analyst II ............................................................................... 39
22. Malware Detection Analyst III ............................................................................... 39
23. Malware Detection Analyst IV ............................................................................... 40
24. Malware Detection – Manager/Lead ....................................................................... 40
25. Threat Intelligence Analyst I .................................................................................. 40
26. Threat Intelligence Analyst II ................................................................................ 41
27. Threat Intelligence Analyst – Manager/Lead ......................................................... 41
28. Risk and Vulnerability Assessment Team - Principal ............................................ 42
29. Risk and Vulnerability Assessment Team – Subject Matter Expert (SME) .......... 42
30. Security Controls Assessment Analyst I ............................................................... 42
31. Security Controls Assessment Analyst II ............................................................. 42
32. Security Controls Assessment Analyst IV ............................................................. 43
33. Information Assurance Engineer I ......................................................................... 43
34. Information Assurance Engineer II ........................................................................ 43
35. Information Assurance Engineer III ....................................................................... 43
36. Information Assurance Policy Analyst ................................................................. 44
37. Senior Information Assurance Policy Analyst ....................................................... 44
38. Information Assurance Subject Matter Expert (SME) .......................................... 44
39. Vulnerability Management Analyst I .................................................................... 45
40. Vulnerability Management Analyst II ................................................................... 45
41. Vulnerability Management Analyst III ................................................................. 46
42. Vulnerability Management Analyst IV ................................................................. 46
43. Vulnerability Management Analyst – Manager/Lead .......................................... 47
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS
PREAMBLE ................................................................................................................. 48
BLANKET PURCHASE AGREEMENT I - FEDERAL SUPPLY SCHEDULE ......................... 49
BLANKET PURCHASE AGREEMENT II ................................................................... 50
CONTRACTOR TEAM ARRANGEMENTS .................................................................... 51
INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS

SPECIAL NOTICE TO AGENCIES: Small Business Participation
SBA strongly supports the participation of small business concerns in the Federal Supply Schedules Program. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micro purchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage! online shopping service (www.fss.gsa.gov). The catalogs/pricelists, GSA Advantage! and the Federal Supply Service Home Page (www.fss.gsa.gov) contains information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micro purchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1. GEOGRAPHIC SCOPE OF CONTRACT:

Domestic delivery 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.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

Offerors are requested to check one of the following boxes:
[X] The Geographic Scope of Contract will be domestic and overseas delivery.
[ ] The Geographic Scope of Contract will be overseas delivery only.
[ ] The Geographic Scope of Contract will be domestic delivery only.

2. CONTRACTOR’S ORDERING AND PAYMENT INFORMATION:

<table>
<thead>
<tr>
<th>ORDERING INFORMATION</th>
<th>PAYMENT INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacobs Technology Inc.</td>
<td>Jacobs Technology Inc.</td>
</tr>
<tr>
<td>Attention: Darin Williams</td>
<td>Attention: Accounts Receivable</td>
</tr>
<tr>
<td>600 William Northern Blvd.</td>
<td>PO Box 409767</td>
</tr>
<tr>
<td>Tullahoma, TN 37388-4729</td>
<td>Atlanta, GA 30384-9767</td>
</tr>
<tr>
<td>Phone: (610) 238-1009</td>
<td>Point of Contact: Angelia Nelson</td>
</tr>
<tr>
<td>Fax: (931) 393-6210</td>
<td>Phone: (931) 393-6471</td>
</tr>
<tr>
<td>Email Address: <a href="mailto:Darin.Williams@jacobs.com">Darin.Williams@jacobs.com</a></td>
<td>Email Address: <a href="mailto:Angelia.Nelson@jacobs.com">Angelia.Nelson@jacobs.com</a></td>
</tr>
</tbody>
</table>

Contractor must accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract. The Contractor and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold (See GSAR 552.232-79 Payment by Credit Card). In addition, bank account information for wire transfer payments will be shown on the invoice.

The following telephone number can be used by ordering agencies to obtain technical and/or ordering assistance: Office: (703) 896-4000
3. 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.

4. STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279:

Block 9: G. Order/Modification under Federal Schedule
Block 16: Data Universal Numbering System (DUNS) Number: 00-792-3014
Block 30: Type of Contractor: Large Business
Block 31: Woman-Owned Small Business: No
Block 37: Contractor Taxpayer Identification Number (TIN): 62-0510412
Block 40: Veteran Owned Small Business (VOSB): No

4a. CAGE Code: 07486
4b. Contractor has registered with: System Award Management www.sam.gov

5. FOB DESTINATION (CONUS AND OCONUS)

The Contractor shall conform to FOB Destination requirements at the request of the ordering agency. Please note that Contractor primarily provides services.

Not applicable to Services.

6. DELIVERY SCHEDULE

a. TIME OF DELIVERY: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>45 Days or as stated on the Order</td>
</tr>
<tr>
<td>54151HACS</td>
<td>45 Days or as stated on the Order</td>
</tr>
<tr>
<td>OLM</td>
<td>30 Days or as stated on the Order</td>
</tr>
</tbody>
</table>

b. 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.

7. DISCOUNTS:

Prices shown are NET Prices; Basic Discounts have been deducted.

a. Prompt Payment: None
b. Quantity: None
c. Dollar Volume: None
d. Government Educational Institutions: None
e. Other: None

8. 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.

9. **STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING:**

Not applicable

10. **SMALL REQUIREMENTS:**

The minimum dollar value of orders to be issued is $100.00.

11. **MAXIMUM ORDER:**

(All dollar amounts are exclusive of any discount for prompt payment.)

a. The Maximum Order value for the following Special Item Numbers (SINs) is $500,000:
   - Special Item Number 54151HACS – Highly Adaptive Cybersecurity Services (HACS)
   - Special Item Number 54151S – Information Technology (IT) Professional Services

b. The Maximum Order value for the following Special Item Number (SIN) is $250,000:
   - Special Item Number 70-500 – Order-Level Materials

12. **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.

13. **FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION 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.

13.1. **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.
13.2. FEDERAL TELECOMMUNICATION STANDARDS (FED-STD):

Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STD) 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.

14. CONTRACT OR TASKS/ SPECIAL REQUIREMENTS:

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).

15. CONTRACT ADMINISTRATION FOR ORDERING OFFICES:

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)

16. GSA Advantage!

GSA Advantage! is online, interactive electronic information and ordering system that provides online 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:

(1) Manufacturer;
(2) Manufacturer's Part Number; and
(3) Product categories.

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

17. 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-

(1) 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));
(2) The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;
(3) The items are clearly labeled on the order as items not on the Federal Supply Schedule; and
(4) All clauses applicable to items not on the Federal Supply Schedule are included in the order.

18. 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.

Jacobs Technology Inc.
Contract Number 47QTCA20D001R
Page 5
(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.

19. 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.

20. 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).

21. 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.

22. INSTALLATION, DE-INSTALLATION, 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 apply.

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, de-installation, and reinstallation services under SIN 132-8 or 132-9.

23. SECTION 508 COMPLIANCE
If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following:

The EIT standard can be found at:  www.Section508.gov/.

24. **INSURANCE-WORK ON A GOVERNMENT INSTALLATION (JAN 1997) (FAR 52.228-5)28.310**

   (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.

25. **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.

26. **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)

27. **ORDER-LEVEL MATERIALS**

   (a) This Schedule is authorized to allow for order-level materials (OLMs) in accordance with GSAR 538.7201. A listing of all OLM-authorized Schedules is available at www.gsa.gov/olm.

   (b) Clauses 552.212-4 Contract Terms and Conditions - Alternate I and 552.238-82 Special Ordering Procedures for the Acquisition of Order-Level Materials provide additional information on inclusion of OLMs in task and delivery orders placed against a Federal Supply Schedule (FSS) contract or FSS blanket purchase agreement (BPA).

   (c) OLMs are only authorized for inclusion at the order level under a Time-and-Materials (T&M) or Labor-Hour (LH) Contract Line Item Number (CLIN) and are subject to a Not To Exceed (NTE) ceiling price.
(d) Offerors proposing the Order-Level Materials Special Item Number (SIN) are not required to propose items or pricing at the contract level, since by definition OLMs are unknown at the time of FSS contract award. The ordering activity contracting officer is responsible for defining OLMs and determining proposed OLM pricing fair and reasonable for a particular order.

(e) OLMs are purchased under the authority of the FSS Program and are not “open market items.”

(f) Items awarded under ancillary supplies/services and other direct cost (ODC) SINs are not OLMs. These SINs are reserved for items that can be defined and priced up-front at the FSS contract level.

(g) The Order-Level Materials SIN cannot be the only SIN awarded on a contract. The Order-Level Materials SIN is only authorized for use in direct support of another awarded SIN.

(h) The Order-Level Materials SIN is exempt from CSP-1 Commercial Sales Practices disclosure requirements.

(i) The Order-Level Materials SIN is exempt from the following clauses:

552.216-70 Economic Price Adjustment - FSS Multiple Award Schedule Contracts
I-FSS-969 Economic Price Adjustment - FSS Multiple Award Schedule
552.238-71 Submission and Distribution of Authorized FSS Schedule Pricelists
552.238-75 Price Reductions

(j) Terms and conditions that otherwise apply to the FSS contract also apply to the Order-Level Materials SIN. Examples include but are not limited to:

- Trade Agreements Act (TAA)
- Sales reporting and Industrial Funding Fee (IFF) remittance
- Environmental Attributes clauses
- AbilityOne Program Essentially the Same (ETS) compliance

(k) Prices for items provided under the Order-Level Materials SIN must be inclusive of the IFF. The value of order-level materials in a task or delivery order [or the cumulative value of order-level materials in orders against an FSS BPA] awarded under an FSS contract, shall not exceed 33.33%.

(l) There are no administrative, technical, or price proposal requirements for the Order-Level Materials SIN (i.e., Section I - Administrative/Contract Data, Section II - Technical Proposal, and Section III - Price Proposal). The Order-Level Materials SIN will be awarded when proposed by an offeror, provided that (1) the Schedule is authorized for inclusion of OLMs, and (2) the Order-Level Materials SIN will not be the only awarded SIN under the contract.
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S)

1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Services within the scope of this 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 in accordance with this clause.
   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) (DEVIA TION 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) (DEVIA TION 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;
13. **RESUMES**

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

14. **INCIDENTAL SUPPORT COSTS**

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

15. **APPROVAL OF SUBCONTRACTS**

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

16. **DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING**

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

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

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

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

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

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

Minimum Education: Bachelor's Degree in Computer Science
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-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (PII)
- OMB Memorandum M-19-03 - Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
- 2017 Report to the President on Federal IT Modernization
- The Cybersecurity National Action Plan (CNAP)
- NIST SP 800-14 - Generally Accepted Principles and Practices for Securing Information Technology Systems
- NIST SP 800-27A - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- NIST SP 800-30 - Guide for Conducting Risk Assessments
- NIST SP 800-35 - Guide to Information Technology Security Services
- NIST SP 800-44 - Guidelines on Securing Public Web Servers
- NIST SP 800-48 - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-61 - Computer Security Incident Handling Guide
- NIST SP 800-64 - Security Considerations in the System Development Life Cycle
- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-86 - Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-115 - Technical Guide to Information Security Testing and Assessment
- NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs)
- NIST SP 800-171 - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE

   a. The labor categories, prices, terms, and conditions stated under Special Item Number 54151HACS Highly Adaptive Cybersecurity Services (HACS) apply exclusively to Highly Adaptive Cybersecurity Services within the scope of this Schedule.

   b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on the MAS Schedule, and may be quoted along with services to provide a total solution.

   c. This SIN provides ordering activities with access to Highly Adaptive Cybersecurity services only.

   d. Highly Adaptive Cybersecurity Services provided under this SIN shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.
e. SCOPE:

54151HACS Highly Adaptive Cybersecurity Services (HACS) - SUBJECT TO COOPERATIVE PURCHASING
- includes proactive and reactive cybersecurity services that improve the customer’s enterprise-level security posture.

The scope of this category encompasses a wide range of fields that include, but are not limited to, Risk Management Framework (RMF) services, information assurance (IA), virus detection, network management, situational awareness and incident response, secure web hosting, and backup and security services.

The seven-step RMF includes preparation, information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. RMF activities may also include Information Security Continuous Monitoring Assessment (ISCMAs) which evaluate organization-wide ISCM implementations, and also Federal Incident Response Evaluations (FIREs), which assess an organization’s incident management functions.

The scope of this category also includes Security Operations Center (SOC) services. The SOC scope includes services such as: 24x7x365 monitoring and analysis, traffic analysis, incident response and coordination, penetration testing, anti-virus management, intrusion detection and prevention, and information sharing.

HACS vendors are able to identify and protect a customer’s information resources, detect and respond to cybersecurity events or incidents, and recover capabilities or services impaired by any incidents that emerge.

Sub-Categories

● High Value Asset (HVA) Assessments include Risk and Vulnerability Assessment (RVA) which assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA subcategory include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing. Security Architecture Review (SAR) evaluates a subset of the agency’s HVA security posture to determine whether the agency has properly architected its cybersecurity solutions and ensures that agency leadership fully understands the risks inherent in the implemented cybersecurity solution. The SAR process utilizes in-person interviews, documentation reviews, and leading practice evaluations of the HVA environment and supporting systems. SAR provides a holistic analysis of how an HVA’s individual security components integrate and operate, including how data is protected during operations. Systems Security Engineering (SSE) identifies security vulnerabilities and minimizes or contains risks associated with these vulnerabilities spanning the Systems Development Life Cycle. SSE focuses on, but is not limited to the following security areas: perimeter security, network security, endpoint security, application security, physical security, and data security.

● Risk and Vulnerability Assessment (RVA) assesses threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations. The services offered in the RVA sub-category include Network Mapping, Vulnerability Scanning, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), Database Assessment, and Penetration Testing.

● Cyber Hunt activities respond to crises or urgent situations within the pertinent domain to mitigate immediate and potential threats. Cyber Hunts start with the premise that threat actors known to target some organizations in a specific industry or with specific systems are likely to also target other organizations in the same industry or with the same systems.
• 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.

• 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.

f. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. ORDER

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

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

3. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.

b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.

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

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

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS– COMMERCIAL ITEMS (Jan 2017) & (ALTERNATE I-Jan 2017) for Time-and-Materials and Labor-Hour orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR

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

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

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

“Contractor and its affiliates” and “Contractor or its affiliates” 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

a. The Contractor shall provide a description of the Highly Adaptive Cybersecurity Service offered under Special Item Numbers 54151HACS for Highly Adaptive Cybersecurity Services and it should be

Jacobs Technology Inc.
Contract Number 47QTCA20D001R
Page 16
presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.
<table>
<thead>
<tr>
<th>SITE</th>
<th>SIN</th>
<th>5415S IT PROFESSIONAL SERVICES</th>
<th>RATE YEAR 1</th>
<th>RATE YEAR 2</th>
<th>RATE YEAR 3</th>
<th>RATE YEAR 4</th>
<th>RATE YEAR 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>5415S</td>
<td>Administrative Support</td>
<td>$ 40.90</td>
<td>$ 42.00</td>
<td>$ 43.13</td>
<td>$ 44.29</td>
<td>$ 45.49</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Analyst</td>
<td>$ 122.12</td>
<td>$ 125.42</td>
<td>$ 128.81</td>
<td>$ 132.29</td>
<td>$ 135.86</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Business Analyst I</td>
<td>$ 62.75</td>
<td>$ 64.44</td>
<td>$ 66.18</td>
<td>$ 67.97</td>
<td>$ 69.81</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Business Analyst II</td>
<td>$ 72.52</td>
<td>$ 74.48</td>
<td>$ 76.49</td>
<td>$ 78.56</td>
<td>$ 80.68</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Consultant I</td>
<td>$ 140.26</td>
<td>$ 144.05</td>
<td>$ 147.94</td>
<td>$ 151.93</td>
<td>$ 156.03</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Consultant II</td>
<td>$ 192.86</td>
<td>$ 198.07</td>
<td>$ 203.42</td>
<td>$ 208.91</td>
<td>$ 214.55</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Consultant III</td>
<td>$ 216.23</td>
<td>$ 222.07</td>
<td>$ 228.07</td>
<td>$ 234.23</td>
<td>$ 240.55</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Help Desk Operator</td>
<td>$ 70.13</td>
<td>$ 72.02</td>
<td>$ 73.96</td>
<td>$ 75.96</td>
<td>$ 78.01</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Engineer</td>
<td>$ 157.79</td>
<td>$ 162.05</td>
<td>$ 166.43</td>
<td>$ 170.92</td>
<td>$ 175.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Network Engineer</td>
<td>$ 111.04</td>
<td>$ 114.04</td>
<td>$ 117.12</td>
<td>$ 120.28</td>
<td>$ 123.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Network Operating Center Technician</td>
<td>$ 75.97</td>
<td>$ 78.02</td>
<td>$ 80.13</td>
<td>$ 82.29</td>
<td>$ 84.51</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Principal/Partner</td>
<td>$ 262.98</td>
<td>$ 270.08</td>
<td>$ 277.37</td>
<td>$ 284.86</td>
<td>$ 292.55</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Program Manager</td>
<td>$ 210.39</td>
<td>$ 216.07</td>
<td>$ 221.90</td>
<td>$ 227.89</td>
<td>$ 234.04</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Programmer/Analyst I</td>
<td>$ 111.04</td>
<td>$ 114.04</td>
<td>$ 117.12</td>
<td>$ 120.28</td>
<td>$ 123.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Programmer/Analyst II</td>
<td>$ 134.41</td>
<td>$ 138.04</td>
<td>$ 141.77</td>
<td>$ 145.60</td>
<td>$ 149.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Programmer/Analyst III</td>
<td>$ 171.14</td>
<td>$ 175.76</td>
<td>$ 180.51</td>
<td>$ 185.38</td>
<td>$ 190.39</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Project Manager</td>
<td>$ 175.33</td>
<td>$ 180.06</td>
<td>$ 184.92</td>
<td>$ 189.91</td>
<td>$ 195.04</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Quality Assurance/Test Engineer</td>
<td>$ 78.94</td>
<td>$ 81.07</td>
<td>$ 83.26</td>
<td>$ 85.51</td>
<td>$ 87.82</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Security Engineer</td>
<td>$ 134.41</td>
<td>$ 138.04</td>
<td>$ 141.77</td>
<td>$ 145.60</td>
<td>$ 149.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Senior Systems Architect</td>
<td>$ 239.61</td>
<td>$ 246.08</td>
<td>$ 252.72</td>
<td>$ 259.54</td>
<td>$ 266.55</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Software Architect</td>
<td>$ 181.16</td>
<td>$ 186.05</td>
<td>$ 191.07</td>
<td>$ 196.23</td>
<td>$ 201.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>System Administrator</td>
<td>$ 116.89</td>
<td>$ 120.05</td>
<td>$ 123.29</td>
<td>$ 126.62</td>
<td>$ 130.04</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Systems Engineer</td>
<td>$ 111.04</td>
<td>$ 114.04</td>
<td>$ 117.12</td>
<td>$ 120.28</td>
<td>$ 123.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Technical Writer</td>
<td>$ 99.35</td>
<td>$ 102.03</td>
<td>$ 104.78</td>
<td>$ 107.61</td>
<td>$ 110.52</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Telecom Engineer I</td>
<td>$ 87.66</td>
<td>$ 90.03</td>
<td>$ 92.46</td>
<td>$ 94.96</td>
<td>$ 97.52</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Telecom Engineer II</td>
<td>$ 99.35</td>
<td>$ 102.03</td>
<td>$ 104.78</td>
<td>$ 107.61</td>
<td>$ 110.52</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Telecom Engineer III</td>
<td>$ 111.04</td>
<td>$ 114.04</td>
<td>$ 117.12</td>
<td>$ 120.28</td>
<td>$ 123.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Assurance Engineer I</td>
<td>$ 105.19</td>
<td>$ 108.03</td>
<td>$ 110.95</td>
<td>$ 113.95</td>
<td>$ 117.03</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Assurance Engineer II</td>
<td>$ 157.79</td>
<td>$ 162.05</td>
<td>$ 166.43</td>
<td>$ 170.92</td>
<td>$ 175.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Assurance Engineer III</td>
<td>$ 187.01</td>
<td>$ 192.06</td>
<td>$ 197.25</td>
<td>$ 202.58</td>
<td>$ 208.05</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Assurance Policy Analyst</td>
<td>$ 163.64</td>
<td>$ 168.06</td>
<td>$ 172.60</td>
<td>$ 177.26</td>
<td>$ 182.05</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Senior Information Assurance Policy Analyst</td>
<td>$ 204.34</td>
<td>$ 210.06</td>
<td>$ 215.73</td>
<td>$ 221.55</td>
<td>$ 227.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Information Assurance Subject Matter Expert</td>
<td>$ 257.15</td>
<td>$ 264.09</td>
<td>$ 271.22</td>
<td>$ 278.54</td>
<td>$ 286.06</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Senior Systems Administrator</td>
<td>$ 140.26</td>
<td>$ 144.05</td>
<td>$ 147.94</td>
<td>$ 151.93</td>
<td>$ 156.03</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Program Control Specialist</td>
<td>$ 129.03</td>
<td>$ 132.51</td>
<td>$ 136.09</td>
<td>$ 139.76</td>
<td>$ 143.53</td>
</tr>
<tr>
<td>G</td>
<td>5415S</td>
<td>Senior Administrative Support</td>
<td>$ 58.44</td>
<td>$ 60.02</td>
<td>$ 61.64</td>
<td>$ 63.30</td>
<td>$ 65.01</td>
</tr>
</tbody>
</table>
## SIN 54151S – CONTRACTOR SITE IT PROFESSIONAL SERVICES LABOR RATES

<table>
<thead>
<tr>
<th>SITE</th>
<th>SIN 54151S IT PROFESSIONAL SERVICES</th>
<th>RATE YEAR 1</th>
<th>RATE YEAR 2</th>
<th>RATE YEAR 3</th>
<th>RATE YEAR 4</th>
<th>RATE YEAR 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Administrative Support</td>
<td>$43.63</td>
<td>$44.81</td>
<td>$46.02</td>
<td>$47.26</td>
<td>$48.54</td>
</tr>
<tr>
<td>C</td>
<td>Analyst</td>
<td>$129.52</td>
<td>$133.01</td>
<td>$136.60</td>
<td>$140.29</td>
<td>$144.08</td>
</tr>
<tr>
<td>C</td>
<td>Business Analyst I</td>
<td>$66.55</td>
<td>$68.35</td>
<td>$70.20</td>
<td>$72.10</td>
<td>$74.05</td>
</tr>
<tr>
<td>C</td>
<td>Business Analyst II</td>
<td>$76.91</td>
<td>$78.99</td>
<td>$81.12</td>
<td>$83.31</td>
<td>$85.56</td>
</tr>
<tr>
<td>C</td>
<td>Consultant I</td>
<td>$149.59</td>
<td>$153.63</td>
<td>$157.78</td>
<td>$162.04</td>
<td>$166.42</td>
</tr>
<tr>
<td>C</td>
<td>Consultant II</td>
<td>$205.68</td>
<td>$211.23</td>
<td>$216.93</td>
<td>$222.79</td>
<td>$228.81</td>
</tr>
<tr>
<td>C</td>
<td>Consultant III</td>
<td>$230.62</td>
<td>$236.85</td>
<td>$243.24</td>
<td>$249.81</td>
<td>$256.55</td>
</tr>
<tr>
<td>C</td>
<td>Help Desk Operator</td>
<td>$74.80</td>
<td>$76.82</td>
<td>$78.89</td>
<td>$81.02</td>
<td>$83.21</td>
</tr>
<tr>
<td>C</td>
<td>Information Engineer</td>
<td>$168.28</td>
<td>$172.82</td>
<td>$177.49</td>
<td>$182.28</td>
<td>$187.20</td>
</tr>
<tr>
<td>C</td>
<td>Network Engineer</td>
<td>$118.43</td>
<td>$121.63</td>
<td>$124.91</td>
<td>$128.28</td>
<td>$131.74</td>
</tr>
<tr>
<td>C</td>
<td>Network Operating Center Technician</td>
<td>$81.03</td>
<td>$83.22</td>
<td>$85.47</td>
<td>$87.78</td>
<td>$90.15</td>
</tr>
<tr>
<td>C</td>
<td>Principal/Partner</td>
<td>$280.48</td>
<td>$288.05</td>
<td>$295.83</td>
<td>$303.82</td>
<td>$312.02</td>
</tr>
<tr>
<td>C</td>
<td>Program Manager</td>
<td>$224.39</td>
<td>$230.45</td>
<td>$236.67</td>
<td>$243.06</td>
<td>$249.62</td>
</tr>
<tr>
<td>C</td>
<td>Programmer/Analyst I</td>
<td>$111.88</td>
<td>$114.90</td>
<td>$118.00</td>
<td>$121.19</td>
<td>$124.46</td>
</tr>
<tr>
<td>C</td>
<td>Programmer/Analyst II</td>
<td>$135.43</td>
<td>$139.09</td>
<td>$142.85</td>
<td>$146.71</td>
<td>$150.67</td>
</tr>
<tr>
<td>C</td>
<td>Programmer/Analyst III</td>
<td>$182.53</td>
<td>$187.46</td>
<td>$192.52</td>
<td>$197.72</td>
<td>$203.06</td>
</tr>
<tr>
<td>C</td>
<td>Project Manager</td>
<td>$182.25</td>
<td>$187.17</td>
<td>$192.22</td>
<td>$197.41</td>
<td>$202.74</td>
</tr>
<tr>
<td>C</td>
<td>Quality Assurance/Test Engineer</td>
<td>$83.72</td>
<td>$85.98</td>
<td>$88.30</td>
<td>$90.68</td>
<td>$93.13</td>
</tr>
<tr>
<td>C</td>
<td>Security Engineer</td>
<td>$143.36</td>
<td>$147.23</td>
<td>$151.21</td>
<td>$155.29</td>
<td>$159.48</td>
</tr>
<tr>
<td>C</td>
<td>Senior Systems Architect</td>
<td>$255.55</td>
<td>$262.45</td>
<td>$269.54</td>
<td>$276.82</td>
<td>$284.29</td>
</tr>
<tr>
<td>C</td>
<td>Software Architect</td>
<td>$188.32</td>
<td>$193.40</td>
<td>$198.62</td>
<td>$203.98</td>
<td>$209.49</td>
</tr>
<tr>
<td>C</td>
<td>System Administrator</td>
<td>$124.66</td>
<td>$128.03</td>
<td>$131.49</td>
<td>$135.04</td>
<td>$138.69</td>
</tr>
<tr>
<td>C</td>
<td>Systems Engineer</td>
<td>$118.43</td>
<td>$121.63</td>
<td>$124.91</td>
<td>$128.28</td>
<td>$131.74</td>
</tr>
<tr>
<td>C</td>
<td>Technical Writer</td>
<td>$105.96</td>
<td>$108.82</td>
<td>$111.76</td>
<td>$114.78</td>
<td>$117.88</td>
</tr>
<tr>
<td>C</td>
<td>Telecom Engineer I</td>
<td>$93.49</td>
<td>$96.01</td>
<td>$98.60</td>
<td>$101.26</td>
<td>$103.99</td>
</tr>
<tr>
<td>C</td>
<td>Telecom Engineer II</td>
<td>$105.96</td>
<td>$108.82</td>
<td>$111.76</td>
<td>$114.78</td>
<td>$117.88</td>
</tr>
<tr>
<td>C</td>
<td>Telecom Engineer III</td>
<td>$118.43</td>
<td>$121.63</td>
<td>$124.91</td>
<td>$128.28</td>
<td>$131.74</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Engineer I</td>
<td>$112.19</td>
<td>$115.22</td>
<td>$118.33</td>
<td>$121.52</td>
<td>$124.80</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Engineer II</td>
<td>$164.02</td>
<td>$168.45</td>
<td>$173.00</td>
<td>$177.67</td>
<td>$182.47</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Engineer III</td>
<td>$199.46</td>
<td>$204.85</td>
<td>$210.38</td>
<td>$216.06</td>
<td>$221.89</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Policy Analyst</td>
<td>$173.50</td>
<td>$178.18</td>
<td>$182.99</td>
<td>$187.93</td>
<td>$193.00</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Policy Analyst</td>
<td>$218.15</td>
<td>$224.04</td>
<td>$230.09</td>
<td>$236.30</td>
<td>$242.68</td>
</tr>
<tr>
<td>C</td>
<td>Information Assurance Subject Matter Expert</td>
<td>$274.24</td>
<td>$281.64</td>
<td>$289.24</td>
<td>$297.05</td>
<td>$305.07</td>
</tr>
<tr>
<td>C</td>
<td>Senior Systems Administrator</td>
<td>$149.59</td>
<td>$153.63</td>
<td>$157.78</td>
<td>$162.04</td>
<td>$166.42</td>
</tr>
<tr>
<td>C</td>
<td>Program Control Specialist</td>
<td>$136.85</td>
<td>$140.54</td>
<td>$144.33</td>
<td>$148.23</td>
<td>$152.23</td>
</tr>
<tr>
<td>C</td>
<td>Senior Administrative Support</td>
<td>$62.33</td>
<td>$64.01</td>
<td>$65.74</td>
<td>$67.51</td>
<td>$69.33</td>
</tr>
</tbody>
</table>
## SIN 54151HACS – GOVERNMENT SITE HACS LABOR RATES

<table>
<thead>
<tr>
<th>SITE</th>
<th>SIN</th>
<th>54151HACS HIGHLY ADAPTIVE CYBER SECURITY SERVICES</th>
<th>RATE</th>
<th>YEAR 1</th>
<th>RATE</th>
<th>YEAR 2</th>
<th>RATE</th>
<th>YEAR 3</th>
<th>RATE</th>
<th>YEAR 4</th>
<th>RATE</th>
<th>YEAR 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Team - Principal</td>
<td>$262.98</td>
<td>$270.08</td>
<td>$277.37</td>
<td>$284.86</td>
<td>$292.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Team - Subject Matter Expert (SME)</td>
<td>$175.33</td>
<td>$180.06</td>
<td>$184.92</td>
<td>$189.91</td>
<td>$195.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Analyst I</td>
<td>$84.65</td>
<td>$86.94</td>
<td>$89.29</td>
<td>$91.70</td>
<td>$94.18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Analyst II</td>
<td>$100.55</td>
<td>$103.26</td>
<td>$106.05</td>
<td>$108.91</td>
<td>$111.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Analyst III</td>
<td>$112.73</td>
<td>$115.77</td>
<td>$118.90</td>
<td>$122.11</td>
<td>$125.41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Analyst IV</td>
<td>$139.32</td>
<td>$143.08</td>
<td>$146.94</td>
<td>$150.91</td>
<td>$154.98</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Penetration Testing Manager/Lead</td>
<td>$157.07</td>
<td>$161.31</td>
<td>$165.67</td>
<td>$170.14</td>
<td>$174.73</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Incident Response Team Principal</td>
<td>$262.98</td>
<td>$270.08</td>
<td>$277.37</td>
<td>$284.86</td>
<td>$292.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Incident Response Team - Subject Matter Expert (SME)</td>
<td>$210.39</td>
<td>$216.07</td>
<td>$221.90</td>
<td>$227.89</td>
<td>$234.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Incident Detection/Response Analyst II</td>
<td>$103.82</td>
<td>$106.62</td>
<td>$109.50</td>
<td>$112.46</td>
<td>$115.50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Incident Detection/Response Analyst III</td>
<td>$128.19</td>
<td>$131.65</td>
<td>$135.20</td>
<td>$138.85</td>
<td>$142.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Incident Detection/Response Analyst IV</td>
<td>$163.54</td>
<td>$167.96</td>
<td>$172.49</td>
<td>$177.15</td>
<td>$181.93</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst I</td>
<td>$66.01</td>
<td>$67.79</td>
<td>$69.62</td>
<td>$71.50</td>
<td>$73.43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst II</td>
<td>$74.83</td>
<td>$76.85</td>
<td>$78.92</td>
<td>$81.05</td>
<td>$83.24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst III</td>
<td>$103.82</td>
<td>$106.62</td>
<td>$109.50</td>
<td>$112.46</td>
<td>$115.50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Analyst IV</td>
<td>$121.65</td>
<td>$124.93</td>
<td>$128.30</td>
<td>$131.76</td>
<td>$135.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Operations Center (SOC) Manager/Lead</td>
<td>$129.72</td>
<td>$133.22</td>
<td>$136.82</td>
<td>$140.51</td>
<td>$144.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Cyber Hunt Team - Principal</td>
<td>$262.98</td>
<td>$270.08</td>
<td>$277.37</td>
<td>$284.86</td>
<td>$292.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Cyber Hunt Team - Subject Matter Expert (SME)</td>
<td>$175.33</td>
<td>$180.06</td>
<td>$184.92</td>
<td>$189.91</td>
<td>$195.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Malware Detection Analyst II</td>
<td>$102.70</td>
<td>$105.47</td>
<td>$108.32</td>
<td>$111.24</td>
<td>$114.24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Malware Detection Analyst III</td>
<td>$121.65</td>
<td>$124.93</td>
<td>$128.30</td>
<td>$131.76</td>
<td>$135.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Malware Detection Analyst IV</td>
<td>$144.78</td>
<td>$148.69</td>
<td>$152.70</td>
<td>$156.82</td>
<td>$161.05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Malware Detection - Manager/Lead</td>
<td>$168.54</td>
<td>$173.09</td>
<td>$177.76</td>
<td>$182.56</td>
<td>$187.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Threat Intelligence Analyst I</td>
<td>$85.34</td>
<td>$87.64</td>
<td>$90.01</td>
<td>$92.44</td>
<td>$94.94</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Threat Intelligence Analyst II</td>
<td>$104.66</td>
<td>$107.49</td>
<td>$110.39</td>
<td>$113.37</td>
<td>$116.43</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Threat Intelligence- Manager/Lead</td>
<td>$176.01</td>
<td>$180.76</td>
<td>$185.64</td>
<td>$190.65</td>
<td>$195.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Risk Vulnerability Assessment (RVA) Team - Principal</td>
<td>$262.98</td>
<td>$270.08</td>
<td>$277.37</td>
<td>$284.86</td>
<td>$292.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Risk Vulnerability Assessment (RVA) Team - Subject Matter Expert</td>
<td>$175.33</td>
<td>$180.06</td>
<td>$184.92</td>
<td>$189.91</td>
<td>$195.04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Controls Assessment Analyst II</td>
<td>$95.28</td>
<td>$97.85</td>
<td>$100.49</td>
<td>$103.20</td>
<td>$105.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Controls Assessment Analyst III</td>
<td>$109.55</td>
<td>$112.51</td>
<td>$115.55</td>
<td>$118.67</td>
<td>$121.87</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Security Controls Assessment Analyst IV</td>
<td>$131.73</td>
<td>$135.29</td>
<td>$138.94</td>
<td>$142.69</td>
<td>$146.54</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Information Assurance Engineer I</td>
<td>$105.19</td>
<td>$108.03</td>
<td>$110.95</td>
<td>$113.95</td>
<td>$117.03</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Information Assurance Engineer II</td>
<td>$157.79</td>
<td>$162.05</td>
<td>$166.43</td>
<td>$170.92</td>
<td>$175.53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Information Assurance Engineer III</td>
<td>$187.01</td>
<td>$192.06</td>
<td>$197.25</td>
<td>$202.58</td>
<td>$208.05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Information Assurance Policy Analyst</td>
<td>$163.64</td>
<td>$168.06</td>
<td>$172.60</td>
<td>$177.26</td>
<td>$182.05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Senior Information Assurance (IA) Policy Analyst</td>
<td>$204.54</td>
<td>$210.06</td>
<td>$215.73</td>
<td>$221.55</td>
<td>$227.53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Information Assurance Subject Matter Expert (SME)</td>
<td>$257.15</td>
<td>$264.09</td>
<td>$271.22</td>
<td>$278.54</td>
<td>$286.06</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Vulnerability Management Analyst I</td>
<td>$95.28</td>
<td>$97.85</td>
<td>$100.49</td>
<td>$103.20</td>
<td>$105.99</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Vulnerability Management Analyst II</td>
<td>$121.98</td>
<td>$125.27</td>
<td>$128.65</td>
<td>$132.12</td>
<td>$135.69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Vulnerability Management Analyst III</td>
<td>$145.56</td>
<td>$149.49</td>
<td>$153.53</td>
<td>$157.68</td>
<td>$161.94</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Vulnerability Management Analyst IV</td>
<td>$179.79</td>
<td>$184.64</td>
<td>$189.63</td>
<td>$194.75</td>
<td>$200.01</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td>54151HACS</td>
<td>Vulnerability Management Analyst - Manager/Lead</td>
<td>$197.36</td>
<td>$202.69</td>
<td>$208.16</td>
<td>$213.78</td>
<td>$219.55</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SITE</td>
<td>SIN</td>
<td>54151HACS HIGHLY ADAPTIVE CYBER SECURITY SERVICES</td>
<td>RATE</td>
<td>RATE</td>
<td>RATE</td>
<td>RATE</td>
<td>RATE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>--------------------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>YEAR 1</td>
<td>YEAR 2</td>
<td>YEAR 3</td>
<td>YEAR 4</td>
<td>YEAR 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Team - Principal</td>
<td>$280.48</td>
<td>$288.05</td>
<td>$295.83</td>
<td>$303.82</td>
<td>$312.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Team - Subject Matter Expert (SME)</td>
<td>$182.25</td>
<td>$187.17</td>
<td>$192.22</td>
<td>$197.41</td>
<td>$202.74</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Analyst I</td>
<td>$89.83</td>
<td>$92.26</td>
<td>$94.75</td>
<td>$97.31</td>
<td>$99.94</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Analyst II</td>
<td>$106.69</td>
<td>$109.57</td>
<td>$112.53</td>
<td>$115.57</td>
<td>$118.69</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Analyst III</td>
<td>$119.61</td>
<td>$122.84</td>
<td>$126.16</td>
<td>$129.57</td>
<td>$133.07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Analyst IV</td>
<td>$147.83</td>
<td>$151.82</td>
<td>$155.92</td>
<td>$160.13</td>
<td>$164.45</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Penetration Testing Manager/Lead</td>
<td>$166.64</td>
<td>$171.14</td>
<td>$175.76</td>
<td>$180.51</td>
<td>$185.38</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Response Team Principal</td>
<td>$280.48</td>
<td>$288.05</td>
<td>$295.83</td>
<td>$303.82</td>
<td>$312.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Response Team - Subject Matter Expert (SME)</td>
<td>$224.39</td>
<td>$230.45</td>
<td>$236.67</td>
<td>$243.06</td>
<td>$249.62</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Detection/Response Analyst II</td>
<td>$79.40</td>
<td>$81.54</td>
<td>$83.74</td>
<td>$86.00</td>
<td>$88.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Detection/Response Analyst III</td>
<td>$110.14</td>
<td>$113.11</td>
<td>$116.16</td>
<td>$119.30</td>
<td>$122.52</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Detection/Response Analyst IV</td>
<td>$136.01</td>
<td>$139.68</td>
<td>$143.45</td>
<td>$147.32</td>
<td>$151.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Incident Detection/Response Manager/Lead</td>
<td>$173.53</td>
<td>$178.22</td>
<td>$183.03</td>
<td>$187.97</td>
<td>$193.05</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Operations Center (SOC) Analyst I</td>
<td>$70.01</td>
<td>$71.90</td>
<td>$73.84</td>
<td>$75.83</td>
<td>$77.88</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Operations Center (SOC) Analyst II</td>
<td>$79.40</td>
<td>$81.54</td>
<td>$83.74</td>
<td>$86.00</td>
<td>$88.32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Operations Center (SOC) Analyst III</td>
<td>$110.14</td>
<td>$113.11</td>
<td>$116.16</td>
<td>$119.30</td>
<td>$122.52</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Operations Center (SOC) Analyst IV</td>
<td>$129.07</td>
<td>$132.55</td>
<td>$136.13</td>
<td>$139.81</td>
<td>$143.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Cyber Hunt Team - Principal</td>
<td>$280.48</td>
<td>$288.05</td>
<td>$295.83</td>
<td>$303.82</td>
<td>$312.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Cyber Hunt Team - Subject Matter Expert (SME)</td>
<td>$182.25</td>
<td>$187.17</td>
<td>$192.22</td>
<td>$197.41</td>
<td>$202.74</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Malware Detection Analyst II</td>
<td>$108.96</td>
<td>$111.90</td>
<td>$114.92</td>
<td>$118.02</td>
<td>$121.21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Malware Detection Analyst III</td>
<td>$129.07</td>
<td>$132.55</td>
<td>$136.13</td>
<td>$139.81</td>
<td>$143.58</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Malware Detection Analyst IV</td>
<td>$153.62</td>
<td>$157.77</td>
<td>$162.03</td>
<td>$166.40</td>
<td>$170.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Malware Detection - Manager/Lead</td>
<td>$178.81</td>
<td>$183.64</td>
<td>$188.60</td>
<td>$193.69</td>
<td>$198.92</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Threat Intelligence Analyst I</td>
<td>$90.56</td>
<td>$93.01</td>
<td>$95.52</td>
<td>$98.10</td>
<td>$100.75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Threat Intelligence Analyst II</td>
<td>$111.04</td>
<td>$114.04</td>
<td>$117.12</td>
<td>$120.28</td>
<td>$123.53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Threat Intelligence- Manager/Lead</td>
<td>$186.74</td>
<td>$191.78</td>
<td>$196.96</td>
<td>$202.28</td>
<td>$207.47</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Risk Vulnerability Assessment (RVA) Team - Principal</td>
<td>$280.48</td>
<td>$288.05</td>
<td>$295.83</td>
<td>$303.82</td>
<td>$312.02</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Risk Vulnerability Assessment (RVA) Team - Subject Matter Expert</td>
<td>$182.25</td>
<td>$187.17</td>
<td>$192.22</td>
<td>$197.41</td>
<td>$202.74</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Controls Assessment Analyst II</td>
<td>$101.09</td>
<td>$103.82</td>
<td>$106.62</td>
<td>$109.50</td>
<td>$112.46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Controls Assessment Analyst III</td>
<td>$116.24</td>
<td>$119.38</td>
<td>$122.60</td>
<td>$125.91</td>
<td>$129.31</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Security Controls Assessment Analyst IV</td>
<td>$139.77</td>
<td>$143.54</td>
<td>$147.42</td>
<td>$151.40</td>
<td>$155.49</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Information Assurance Engineer I</td>
<td>$112.19</td>
<td>$115.22</td>
<td>$118.33</td>
<td>$121.52</td>
<td>$124.80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Information Assurance Engineer II</td>
<td>$164.02</td>
<td>$168.45</td>
<td>$173.00</td>
<td>$177.67</td>
<td>$182.47</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Information Assurance Engineer III</td>
<td>$199.46</td>
<td>$204.85</td>
<td>$210.38</td>
<td>$216.06</td>
<td>$221.89</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Information Assurance Policy Analyst</td>
<td>$173.50</td>
<td>$178.18</td>
<td>$182.99</td>
<td>$187.93</td>
<td>$193.00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Senior Information Assurance (IA) Policy Analyst</td>
<td>$218.15</td>
<td>$224.04</td>
<td>$230.09</td>
<td>$236.30</td>
<td>$242.68</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Information Assurance Subject Matter Expert (SME)</td>
<td>$274.24</td>
<td>$281.64</td>
<td>$289.24</td>
<td>$297.05</td>
<td>$305.07</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Vulnerability Management Analyst I</td>
<td>$101.09</td>
<td>$103.82</td>
<td>$106.62</td>
<td>$109.50</td>
<td>$112.46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Vulnerability Management Analyst II</td>
<td>$129.42</td>
<td>$132.91</td>
<td>$136.50</td>
<td>$140.19</td>
<td>$143.98</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Vulnerability Management Analyst III</td>
<td>$154.45</td>
<td>$158.62</td>
<td>$162.90</td>
<td>$167.30</td>
<td>$171.82</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Vulnerability Management Analyst IV</td>
<td>$190.75</td>
<td>$195.90</td>
<td>$201.19</td>
<td>$206.62</td>
<td>$212.20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>54151HACS Vulnerability Management Analyst - Manager/Lead</td>
<td>$209.40</td>
<td>$215.05</td>
<td>$220.86</td>
<td>$226.82</td>
<td>$232.94</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LABOR CATEGORY QUALIFICATION EQUIVALENCIES

Applies to SINs:
54151S   Information Technology Professional Services
54151HACS  Highly Adaptive Cybersecurity Service SIN

When considering the qualifications of an individual against the minimum requirements of the labor categories, substitutions for the education and experience requirements may be made as shown in the table below.

Allowable Substitutions of Education versus Experience
The minimum education and experience for a labor category will be met when the educational equivalencies in the tables below are considered.

Additional relevant educational achievements in excess of requirements can be substituted for experience requirements:

<table>
<thead>
<tr>
<th>Required Education for the Labor Category</th>
<th>Actual Education Obtained by the Employee</th>
<th>Additional Years of Experience Credited the Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA/MS</td>
<td>Ph.D.</td>
<td>3</td>
</tr>
<tr>
<td>BA/BS</td>
<td>Ph.D.</td>
<td>5</td>
</tr>
<tr>
<td>BA/BS</td>
<td>MA/MS</td>
<td>2</td>
</tr>
<tr>
<td>HS/GED</td>
<td>BA/BS</td>
<td>4</td>
</tr>
</tbody>
</table>

Additional years of experience in excess of requirements can be substituted for educational requirements:

<table>
<thead>
<tr>
<th>Actual Education Obtained by the Employee</th>
<th>Required Education for the Labor Category</th>
<th>Additional Years of Experience Needed for Educational Requirements Equivalency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Some High School</td>
<td>HS/GED</td>
<td>3</td>
</tr>
<tr>
<td>HS/GED</td>
<td>Tech-Inst./Military Train.</td>
<td>2</td>
</tr>
<tr>
<td>HS/GED</td>
<td>BA/BS</td>
<td>4</td>
</tr>
<tr>
<td>HS/GED</td>
<td>MA/MS</td>
<td>No equivalency</td>
</tr>
<tr>
<td>HS/GED</td>
<td>Ph.D.</td>
<td>No equivalency</td>
</tr>
<tr>
<td>BA/BS</td>
<td>MA/MS</td>
<td>2</td>
</tr>
<tr>
<td>BA/BS</td>
<td>Ph.D.</td>
<td>5</td>
</tr>
<tr>
<td>MA/MS</td>
<td>Ph.D.</td>
<td>3</td>
</tr>
</tbody>
</table>
SIN 54151S IT PROFESSIONAL SERVICES LABOR CATEGORY DESCRIPTIONS

1. Administrative Support
   Education: Associate’s Degree or technical/trade school.

   Supports documentation preparation and administrative support efforts. Prepares technical documentation in accordance with applicable Government and industry standards. Supports Program or Project Manager on administrative tasks. Gathers, analyzes, edits, and prepares technical information. Conducts research and ensures the use of proper technical terminology and documentation standards. Translates technical information into readable documents. Assists in the preparation of presentation graphics and supports the development of contract deliverables and reports. Supports administrative contract documentation preparation including resource files, correspondence, schedules and travel documentation.

   Experience: Must have at least 1 year experience of performing administrative functions.

2. Analyst
   Education: Bachelor's degree.

   Provides minimally supervised support for difficult analysis and evaluation assignments. Performs analysis and evaluation of existing or proposed processes, applications, systems, or software. Performs, and/or may direct, project planning, scope, control, management, tracking, or review. Performs analysis and evaluation throughout the process, application, system, or software development life-cycle which includes, but is not limited to: planning, requirements, design, acquisition, development, integration, installation/deployment, performance tuning, testing, or training. Performs, or may direct, document development/preparation at various stages of a project life-cycle (e.g., planning through implementation) to detail analysis results and solution recommendations. May serve as a liaison between functional and technical specialists. Assists with testing to support the project life-cycle, as applicable. Uses methodologies, modeling/estimating techniques, tools, applications, systems, software, or databases at advanced levels to perform assigned tasks. Ensures compliance with, and/or may develop, the standards and organization requirements relative to specific assignments.

   Experience: Must have at least 5 years of relevant experience in an area of specialization associated with the requirement.

3. Business Analyst I
   Education: Bachelor’s degree.

   Meets with customers and/or Contracting Officer’s Representative (COR) and technical staff to coordinate efforts, resolve conflicts, and provide guidance for meeting project requirements. Evaluates proposed automated solutions to determine technical and functional feasibility and adequacy, and cost for implementation and operation. Ensures that functional integration is adequately planned and implemented in order to meet total system requirements. Guides the customer through requirements analysis. Passes requirements to task leaders, reviews design functionality and assists in the planning and execution of system development tasks. Assists with system design, quality assurance, testing and customer training. Prepares and documents briefings. Provides functional area analysis and support for information systems development. Supports the execution of technical tasks, reviews work products for correctness, design specifications, user interface, and schedule and cost compliance. Assists management in mitigating risk and assuring customer satisfaction.

   Experience: Must have at least 3 years of relevant experience.

4. Business Analyst II
   Education: Bachelor’s degree.

   Meets with customers and/or Contracting Officer’s Representative (COR) and technical staff to coordinate efforts, resolve conflicts, and provide guidance for meeting project requirements.
Evaluates proposed automated solutions to determine technical and functional feasibility and adequacy, and cost for implementation and operation. Ensures that functional integration is adequately planned and implemented in order to meet total system requirements. Guides the customer through requirements analysis. Passes requirements to task leaders, reviews design functionality and assists in the planning and execution of system development tasks. Assists with system design, quality assurance, testing and customer training. Prepares and documents briefings. Assists with project management functions, tracking task status and interfacing with customer and/or COR. Provides functional area analysis and support for information systems development. Supports the execution of technical tasks, reviews work products for correctness, design specifications, user interface, and schedule and cost compliance. Assists management in mitigating risk and assuring customer satisfaction.

Experience: Must have at least 6 years of relevant experience.

5. **Consultant I**
Education: Bachelor’s degree.

Provides in-depth knowledge and insight, technical experience and/or subject-matter expertise to help solve complex problems or in support of complex information systems development/support efforts. Performs analyses and develops recommendations that may have substantial impact on programs and activities. Provides in-depth domain expertise to project technical staff and/or customers.

Experience: Must have at least 5 years of relevant experience.

6. **Consultant II**
Education: Bachelor’s degree.

Provides in-depth knowledge and insight, technical experience and/or subject-matter expertise to help solve complex problems or in support of complex information systems development/support efforts. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Provides in-depth domain expertise to project technical staff and/or customers. May supervise technical staff.

Experience: Must have at least 10 years of relevant experience.

7. **Consultant III**
Education: Bachelor’s degree.

Provides in-depth knowledge and insight, technical experience and/or subject-matter expertise to help solve complex problems or in support of complex information systems development/support efforts. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Provides in-depth domain expertise to project technical staff and/or customers. May supervise technical staff.

Experience: Must have at least 15 years of relevant experience.

8. **Help Desk Operator**
Education: High School diploma, Technical Institute Certification, Military Trained.

Under immediate supervision, responds to and diagnoses problems through discussions with users. Conducts problem recognition, research, isolation, resolution, and follow-up steps. Resolves less complex problems immediately and assigns more complex problems to second-level support, senior operator, or supervisor. Assures timely close-out of trouble tickets and escalates additional support as needed.

Experience: Must have at least 1 year experience of performing help desk functions.
9.  **Information Engineer**  
**Education:** Bachelor’s Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.

Performs high level information engineering planning, analysis, design, construction and implementation of complex data-based systems. Develops project plans, controls project scope, and tracks direction in review of complex data products. Designs and facilitates rapid prototyping and joint application development (JAD) sessions designed to provide input into the case tool for development of the application.

**Experience:** Must have at least 6 years of experience with 2 years of experience in application requirements, system development, and implementation. Implementation must include the utilization of I-CASE Information Engineering processes, methodologies, automated I-CASE tools/toolsets, database modeling and design concepts.

10.  **Network Engineer**  
**Education:** A Bachelor’s degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline.

Responsible for acquisition, installation, maintenance, and usage of network hardware and software. Determines products to meet needs and presents results. Manages system performance and maintains system security. Troubleshoots system problems. Establishes and implements system policies, procedures, and standards, and ensures their conformance with information systems objectives. May train users on system operation. May perform network planning and engineering functions. May be responsible for both local and remote administration of networks.

**Experience:** Must have at least 2 years of technical experience installing, maintaining, and managing Local Area Networks (LANs).

11.  **Network Operating Center Technician**  
**Education:** High School Diploma.

A member of the technical staff who performs monitoring, notification, tracking and problem resolution on enterprise IT services. Works closely with developers and vendors to develop architecture that supports needs. Supports the NOC Manager to ensure that the technology and processes are in place and followed, service interruptions are tracked to resolution, and proper escalation to appropriate personnel including the executive staff is followed. Duties may include a combination of the following: establish system requirement, establish communications paths with system owners, develop test criteria, install equipment at designated site, and/or perform operational tests on equipment and circuits.

**Experience:** Must have at least 1 year of relevant experience.

12.  **Principal / Partner**  
**Education:** Master’s Degree.

Provides consulting and executive support to enterprise-wide or national level programs and personnel. Provides executive knowledge and insight, technical experience and/or subject-matter expertise to projects. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Performs enterprise-wide strategic systems planning. May supervise technical staff.

**Experience:** Must have at least 12 years of experience supporting the resolution of extremely complex systems engineering, computer science, or other related issues or provides in-depth domain expertise.

13.  **Program Manager**  
**Education:** Bachelor’s Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.
Serves as the contractor's single contract manager and authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: Must have 10 years of experience with 8 years of information systems management experience.

14. **Programmer/Analyst III**

Education: Bachelor's Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.

Provides technical guidance and skills in support of information systems development and integration efforts. Performs in a variety of technical areas including systems requirements analysis, data analysis and engineering, systems design, systems development, computer programming, systems testing and deployment, quality assurance, configuration management, and systems documentation. May serve as a technical lead for a task or project. Provides technical and administrative support for information systems development tasks, including execution of technical tasks, the review of work products for correctness, adherence to the design concept and to user standards, and for progress in accordance with schedules. Coordinates with management staff to ensure problem solution and user satisfaction.

Experience: Must have at least 10 years of experience with 6 years of related technical specialized experience.

15. **Programmer/Analyst I**

Education: Bachelor's Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.

Provides technical support for software development and integration efforts. Performs in a variety of technical areas including systems requirements analysis, data analysis and engineering, systems design, systems development, computer programming, systems testing and deployment, quality assurance, configuration management, and systems documentation. Defines the problem and develops system requirements and program specifications. Integrates, tests, and debugs software components. Prepares required documentation including program-level and user-level documentation. Enhances existing software systems. May provide technical database support including: database design; data integration; data standardization; and database management.

Experience: Must have at least 1 year of relevant experience.

16. **Programmer/Analyst II**

Education: Bachelor's Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.

Provides technical support for software development and integration efforts. Performs in a variety of technical areas including systems requirements analysis, data analysis and engineering, systems design, systems development, computer programming, systems testing and deployment, quality assurance, configuration management, and systems documentation. Typically reports to technical lead for a task or project. Defines the problem and develops system requirements and program specifications. Integrates, tests, and debugs software components. Prepares required documentation including program-level and user-level documentation. Enhances existing software systems. May provide technical database support including: database design; data integration; data standardization; and database management.

Experience: Must have at least 5 years of experience with 3 years of related technical specialized experience.
17. **Project Manager**  
**Education:** Bachelor's degree in computer science, management information systems, engineering, or business management is required.

Serves as the project manager for a large or complex information technology project or group of tasks. The project manager ensures the timely and successful performance of the tasks. The project manager usually reports to a program manager but may report directly to the client’s representative. Takes guidance from the Program Manager and is responsible for the overall management of specific tasks/projects. Ensures technical solutions and schedules are implemented in a timely manner.

**Experience:** Must have at least 7 years of experience with 4 years of information systems management experience.

18. **Quality Assurance (QA) / Test Engineer**  
**Education:** Bachelor's degree.

A member of the technical staff responsible for supporting operational and developmental testing. Responsible for development and execution of test plans and procedures. Assists in development of test master plans with developing contractors and customers. May support both the acquisition and user communities to meet testing needs. May serve as test director of test support team to evaluate and document system capabilities as meeting requirements. Will provide test planning support to include test resource plans and test concepts. Will determine data collection requirements and methods and implement collection strategy during test conduct.

**Experience:** Must have at least 6 years of relevant experience, including a sound familiarity with applicable testing tools and evaluation processes. Must possess good oral and written communication skills for direct client interface.

19. **Security Engineer**  
**Education:** Bachelor's degree.

Support for Information Security (INFOSEC) and trusted systems technology. Assists in the analysis and definition of security requirements. Assists in the design, development, testing, and documentation of cryptographic products, trusted networks, database management systems and telecommunications subsystems. Researches, drafts, and provides input regarding information security policies, trusted computing base architectures, and security engineering practices and processes. Assists with certifications and accreditation reviews, security test and evaluations, and may draft associated reports. Supports automated information system security engineering tasks which may include policy development, asset and risk assessment, development of security specifications/architectures/plans, development and/or installation of digital signature systems, support for key and certificate management, implementation/support of trusted computing base, systems certification and accreditation support, and hands-on development and operation of pilot or prototype information security applications. Provides research and initial input for analysis of the current information security architecture and comparative assessments of alternate approaches. Assists in the design, development, debugging, testing, documentation development and maintenance of computer programs for security applications.

**Experience:** Experience will include at least 2 years in the INFOSEC fields of computer security, cryptography, network security, certification/accreditation, and risk analysis.

20. **Senior System Architect**  
**Education:** Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline.

Provides technical direction and expertise in a variety of specialized areas including information systems engineering, systems architecture, systems integration, telecommunications, systems standards, process engineering, systems design and requirements specification. May serve as technical director or as a senior technical staff member. Responsibilities may include a combination of the following: establishes system...
information requirements, designs architecture to include the software, hardware and communications to support the total requirements, evaluates and integrates cross-functional requirements and interfaces, evaluates and defines system requirements, performs enterprise-wide strategic systems planning, provides technical and/or subject-matter expertise to project, and/or may supervise technical staff.

Experience: Must have 12 years of experience with 10 years of related technical specialized experience.

21. **Software Architect**  
**Education:** Bachelor's Degree in Information Systems Engineering, Computer Science, Engineering, Business, or other related field.

Provides technical direction and expertise in a variety of specialized areas including information systems engineering, software systems architecture, systems integration, data integration, enterprise application integration (EAI), systems design and requirements specification. May serve as technical lead or as a senior technical staff member. Responsibilities may include a combination of the following: establishes system information requirements, designs architecture to include the applications, data and services to support the total requirements, evaluates and integrates cross-functional requirements and interfaces, evaluates and defines software requirements, performs enterprise-wide strategic systems planning, provides technical and/or subject-matter expertise to project, and/or may supervise less senior technical staff.

Experience: Must have at least 8 years of experience with 6 years of related technical specialized experience.

22. **System Administrator**  
**Education:** Bachelor's degree.

Under general supervision from senior technical staff and/or project manager, performs analytical, technical, and administrative work in the planning, design, and installation of new and existing computer systems. Works on moderately complex applications. Confers with technical staff members and/or end users to determine types of hardware and software required. Writes programs to fulfill requirements or selects appropriate commercial off-the-shelf (COTS) software and customizes it as necessary. Installs new hardware and maintains existing hardware. May train end users in use of hardware and software. May perform limited routine network administration functions.

Experience: Must have at least 2 years of experience in the evaluation, installation, configuration management, and user support of hardware and software.

23. **Systems Engineer**  
**Education:** Bachelor's Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field.

Supports systems integration efforts involving hardware, software, operating system and communications interoperability. Provides design, development, and implementation support. Provides technical design, programming, testing, and implementation support for operating, communications, and hardware systems integration. Prepares specifications, code, system tests, and documentation in accordance with standards and requirements specifications. May support installation of physical and software components.

Experience: Must have at least 5 years of experience with 3 years of related technical specialized experience.

24. **Technical Writer**  
**Education:** Bachelor's degree

Reviews, edits and prepares support documentation and technical and operations manuals for selected systems and networks, including related hardware and software. Works closely with other technical team members and/or customers to insure complete and accurate system descriptions and required operating procedures are properly captured. Establishes style, formatting, and related "look and feel" standards for document production. Edits and writes technical materials and manuals. Analyze requirements for needed
documentation and completeness. Ensures that technical subject materials are presented clearly and succinctly. Ensures customer deadlines and publication dates are met.

Experience: Previous customer-related experience and at least 2 years of technical writing experience required. Excellent oral and written communication skills are required. Experience and fluency in standard MS Office software is required.

25. **Telecom Engineer I**
   Education: Bachelor's degree.

Provides technical support for difficult assignments in the planning, analysis, design, testing, and troubleshooting of networks or operational systems. Performs systems planning, information planning, and analysis in support of telecommunications support functions, including trouble ticket management, service order entry, and/or configuration management. Tests processes and data models in support of the planning and analysis efforts using both manual and automated tools. Evaluates system problems of workflow, organization, and planning. Performs all work in accordance with established standards.

Experience: Must have at least 1 year of experience in support of telecommunication systems or networks.

26. **Telecom Engineer II**
   Education: Bachelor's degree.

Provides technical support for difficult assignments in the planning, analysis, design, testing, and troubleshooting of networks or operational systems. Performs and/or leads systems planning, information planning, and analysis in support of telecommunications support functions, including trouble ticket management, service order entry, and/or configuration management. Tests processes and data models in support of the planning and analysis efforts using both manual and automated tools. Evaluates system problems of workflow, organization, and planning. Knowledgeable of applicable telecommunications engineering techniques and the use of automated support tools. Performs all work in accordance with established standards.

Experience: At least 3 years of experience in support of telecommunication systems or networks.

27. **Telecom Engineer III**
   Education: Bachelor's degree.

Provides expert technical support and/or leadership for difficult assignments in the planning, analysis, design, testing, and troubleshooting of networks or operational systems. Performs and/or leads systems planning, information planning, and analysis in support of telecommunications support functions, including trouble ticket management, service order entry, and/or configuration management. Tests processes and data models in support of the planning and analysis efforts using both manual and automated tools. Evaluates system problems of workflow, organization, and planning. Supervises that appropriate corrective action is taken. Knowledgeable of applicable telecommunications engineering techniques and the use of automated support tools. Performs all work in accordance with established standards. May supervise or manage tasks/projects.

Experience: Must have at least 5 years of experience in support of telecommunication systems or networks.

28. **Information Assurance Engineer I**
   Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Responsible for supporting Information Assurance engineering teams with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Required basic understanding of approved COTS security analyst tools and government mitigation/compliance checkers. Basic comprehension of FISMA, DIACAP, NIST-800 SPs and DCID 6/3 standards and policy control grouping. Assist in determining products to meet needs and presents results. Supports system performance and maintaining system security, as well
as troubleshooting any system security problems. May be responsible for both local and remote administration of networks.

Experience: Must have at least 2 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN). Certifications (at least one is desirable): MCP, CompTIA-Network +, CompTIA-Security +

29. **Information Assurance Engineer II**

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Responsible for technical information assurance engineering efforts with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Experience in ST&E process and POAM generation. Requires strong understanding of approved COTS security analyst tools and government mitigation/compliance checkers. Strong comprehension of FISMA, DIACAP, NIST-800 SPs and DCID 6/3 standards and policy control grouping. Experience determining products to meet client needs and presenting results. Acts a tier two support engineer during system performance testing. Experience providing tier two support and troubleshooting any system security problems arising from security lockdowns. May be responsible for both local and remote administration of networks.

Experience: Must have 8 years of experience with at least 3 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN) and 3 years of security engineering, system security auditing or system penetration testing. Certifications (at least one is desirable): MCSA/Unix/Linux, CCNA, CompTIA-Network +, CompTIA-Security +, CISSP Certification

30. **Information Assurance Engineer III**

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Responsible for technical information assurance engineering efforts with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Experience in ST&E process and POAM generation. Requires strong understanding of approved COTS security analyst tools and government mitigation/compliance checkers. Strong familiarity with FIPS 199/200, NIST SP 800-37, NIST SP 800-26, NIST SP 800-53, NIST SP 800-18, OMB Circular A-130 Experience determining products to meet client needs and presenting results. Acts a tier three support engineer during system performance testing. Experience providing tier three support & troubleshooting any system security problems arising from security lockdowns. May be responsible for minor customer interface and IA site engineering leadership.

Experience: Must have 10 years of experience with at least 4 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN) and 4 years of security engineering, system security auditing or system penetration testing. Certifications (at least one is desirable): MCSA/MCSE, CCNA/CCNP, CompTIA-Network +, CompTIA-Security +, CISSP

31. **Information Assurance Policy Analyst**

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Provide Information Assurance support in tracking, reporting and providing guidance in FISMA, DIACAP, NIST-800 SPs, ISO: 17799 and DCID 6/3 standards and policy control grouping. Manage and track annual security compliance activities including but not limited to incident response testing, contingency testing, and policy and procedures. Provide updates to Administration of Access Control Program, manage access/ account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Enforcement and re-alignment of security policy with the document change management process Plan of Action and Milestones (POAM), manage and track completion dates for POAM items, assemble remediation packages for POAM items and perform remediation of findings involving security program compliance.
Experience: Must have 6 years of experience with at least 4 years of Information Assurance Policy experience in experience in security administration, evaluation of security/Information Assurance product capabilities, assessment and policy development. Certifications (at least one is desirable): MCSA/MCSE, CCNA/CCNP, CompTIA-Network +, CompTIA-Security +, CISSP

32. Senior Information Assurance Policy Analyst

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Provide Information Assurance expertise in tracking, reporting and providing guidance in FISMA, DIACAP, NIST-800 SPs, ISO: 17799 and DCID 6/3 standards and policy control grouping. Manage and track annual security compliance activities including but not limited to incident response testing, contingency testing, and policy and procedures. Provide updates to Administration of Access Control Program, manage access/account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Prepare certification analysis and reports, develop or review certification test plans, and provide certification recommendations. Enforcement and re-alignment of security policy with the document change management process Plan of Action and Milestones (POAM), manage and track completion dates for POAM items, assemble remediation packages for POAM items and perform remediation of findings involving security program compliance. Develop a security concept of operations from user requirements or source documents that addresses all of the user's functional and security requirements.

Experience: Must have 10 years of experience with at least 7 years of Information Assurance Policy experience in experience in security administration, evaluation of security/Information Assurance product capabilities, assessment and policy development. Certifications (at least one is desirable): MCSA/MCSE, CCNA/CCNP, CompTIA-Network +, CompTIA-Security +, CISSP, CompTIA-Network +, CompTIA-Security +, CISSP Certification

33. Information Assurance Subject Matter Expert

Education: Master's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Provide Information Assurance expertise in tracking, reporting and providing guidance in FISMA, DIACAP, NIST-800 SPs, ISO: 17799 and DCID 6/3 standards and policy control grouping. Provide senior guidance on the development of and acceptance by civilian and defense Government agencies on Information Assurance plans; system evolution; capabilities; compliance with FISMA, DIACAP, DCID, NIST 800 SP, FIPS, and legal or statutory requirements. Serve as advisor to CIO, CTO, CISO, Program Director, Systems Owner, or Operations Managers to develop, implement, and manage Information Assurance as a core competence. Must have extensive experience in design, test, evaluation, certification and accreditation of systems. Must also possess strong background in Cross Domain Solutions and cross contamination avoidance methodologies. Core skill in requirements analysis, requirements writing, development of security architectures, secure network protocols, secure authentication technologies, intrusion detection systems, information assurance standards and policies, and forensic analysis.

Experience: Must have 15 years of experience with at least 10 years of Information Assurance Policy; technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN); or security engineering, system security auditing, or system penetration testing. Certifications (at least one is desirable): MCSA/MCSE, CCNA/CCNP, CompTIA-Network +, CompTIA-Security +, CISSP

34. Senior System Administrator

Education: Bachelor's degree.

Under general direction from senior technical staff and/or project manager, performs analytical, technical, and administrative work in the planning, design, and installation of new and existing computer systems. Supports complex applications and/or IT infrastructure for an organization. Coordinates with technical staff members and/or end users to determine types of hardware and software required. Responsibilities may
involve the automation of maintenance tasks or the selection of appropriate commercial off-the-shelf software and customizing it as necessary. Installs new hardware and maintains existing hardware. May train helpdesk staff and/or end users in use of hardware or software. May perform some network administration functions or coordinate activities with network engineers.

Experience: Must have at least 5 years of experience in the evaluation, installation, configuration management, and user support of hardware and software.

35. Program Control Specialist

Education: Bachelor’s degree.

Supports the project/program manager for a large or complex information technology project or group of tasks. May interact frequently with the client’s representative. Responsibilities may include the creation and updating of a project plan and all artifacts included in that plan. This will involve coordination with senior technical staff on their activities and the impact of this on the project schedule, budget, risk management, progress reporting, etc. Takes direction from the PM responsible for the overall management of the project and shares responsibility with that PM for the quality of the project plan. May be involved in briefing the client’s representative on some aspects of the project.

Experience: Must have at least 4 years of overall work experience with 2 years of experience supporting the management of projects, budget management, or other similar activities that involve tracking and oversight of team efforts.

36. Senior Administrative Support

Education: Associate’s Degree or technical/trade school.

Supports and often leads or supervises documentation preparation and administrative support efforts. Prepares technical documentation in accordance with applicable Government and industry standards. Supports Program or Project Manager on administrative tasks.Gathers, analyzes, edits, and prepares technical information. Conducts research and ensures the use of proper technical terminology and documentation standards. Translates technical information into readable documents.

Assists in the preparation of presentation graphics and supports the development of contract deliverables and reports. Supports administrative contract documentation preparation including resource files, correspondence, schedules and travel documentation.

Experience: Must have at least 4 years of experience of performing administrative functions.
1. **Penetration Testing Team - Principal**

   **Education:** Bachelor's Degree

   Provides consulting and executive support to enterprise-wide or national level programs and personnel. Provides executive knowledge and insight, technical experience and/or subject-matter expertise to projects. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Performs enterprise-wide strategic systems planning. Responsible for the entire Penetration Testing project/program. Ensures that the team is made up of qualified personnel to conduct internal and external network penetration tests, graphical user interface web application penetration tests, web services application penetration tests, and wireless network penetration tests. Responsible overseeing the writing and reviewing of formal penetration test reports documenting the details of a penetration test and all vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Ensures the team works with Security Architects and Security Engineers to gather information and conduct penetration tests. Reviews and processes static source code vulnerability analysis reports for developed applications as directed. Leads the evaluation of commercial and open source tools to be used for the purposes of penetration testing. Maintains demonstrable knowledge of current vulnerability exploitation techniques. Strong understanding of TCP/IP. Mentors junior Penetration Testers as needed. Researches new vulnerabilities and exploits in technologies directly relevant to the client/program.

   **Experience:** 12 years of experience supporting the resolution of extremely complex systems engineering, computer science, or other related issues or provides in-depth domain expertise.

2. **Penetration Testing Team – Subject Matter Expert (SME)**

   **Education:** Bachelor's Degree

   Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

   **Experience:** 8 total experience with at least 4 years of related experience in information technology and/or information security. Certifications (at least one cert preferred)
   - Certified Ethical Hacker (CEH) or equivalent certification
   - Certified Penetration Tester (CPT) or equivalent certification
   - Offensive Security Certified Expert (OSCE) or equivalent certification
   - Offensive Security Exploitation Expert (OSEE) or equivalent certification
   - Offensive Security Web Expert (OSWE) or equivalent certification
   - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification
   - eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) or equivalent certification

3. **Penetration Testing - Analyst I**

   **Education:** Associates Degree

   Conducts internal and external network penetration tests, graphical user interface web application penetration tests, web services application penetration tests, and wireless network penetration tests. Writes and reviews formal penetration test reports documenting the details of a penetration test and vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Submits tickets for remediation of vulnerabilities and potential issues found during penetration tests. Works with Security Architects and Security Engineers to gather information and conduct penetration tests. Supports research efforts for new vulnerabilities and exploits in technologies directly relevant to the client/program.
Experience: 8 total experience with at least 4 years of related experience in information
technology and/or information security. Certifications (at least one cert preferred)
Certified Ethical Hacker (CEH) or equivalent certification
Certified Penetration Tester (CPT) or equivalent certification
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification
eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) or equivalent certification

4. Penetration Testing - Analyst II

Education: Associates Degree

Conducts internal and external network penetration tests, graphical user interface web application penetration
tests, web services application penetration tests, and wireless network penetration tests.
Writes and reviews formal penetration test reports documenting the details of a penetration test and vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Submits tickets for remediation of vulnerabilities and potential issues found during penetration tests. Works with Security Architects and Security Engineers to gather information and conduct penetration tests. Reviews and processes static source code vulnerability analysis reports for developed applications as directed. Supports evaluation of commercial and open source tools to be used for the purposes of penetration testing. Maintains demonstrable knowledge of current vulnerability exploitation techniques. Understanding of TCP/IP. Supports research of new vulnerabilities and exploits in technologies directly relevant to the client/program.

Experience: 8 total experience with at least 4 years of related experience in information
technology and/or information security. Certifications (at least one cert preferred)
Certified Ethical Hacker (CEH) or equivalent certification
Certified Penetration Tester (CPT) or equivalent certification
Offensive Security Certified Expert (OSCE) or equivalent certification
Offensive Security Exploitation Expert (OSEE) or equivalent certification
Offensive Security Web Expert (OSWE) or equivalent certification
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification
eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) or equivalent certification

5. Penetration Testing - Analyst III

Education: Associates Degree

Conducts internal and external network penetration tests, graphical user interface web application penetration
tests, web services application penetration tests, and wireless network penetration tests. Writes and reviews
formal penetration test reports documenting the details of a penetration test and vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Submits tickets for remediation of vulnerabilities and potential issues found during penetration tests. Works with Security Architects and Security Engineers to gather information and conduct penetration tests. Reviews and processes static source code vulnerability analysis reports for developed applications as directed. Supports evaluation of commercial and open source tools to be used for the purposes of penetration testing. Maintains demonstrable knowledge of current vulnerability exploitation techniques. Strong understanding of TCP/IP. Researches new vulnerabilities and exploits in technologies directly relevant to the client/program.

Experience: 8 total experience with at least 4 years of related experience in information technology
and/or information security. Certifications (at least one cert preferred)
Certified Ethical Hacker (CEH) or equivalent certification
Certified Penetration Tester (CPT) or equivalent certification
Offensive Security Certified Expert (OSCE) or equivalent certification
Offensive Security Exploitation Expert (OSEE) or equivalent certification
Offensive Security Web Expert (OSWE) or equivalent certification
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification

Jacobs Technology Inc.
Contract Number 47QTCA20D001R
Page 34
6. **Penetration Testing - Analyst IV**  
**Education:** Associates Degree

Conducts internal and external network penetration tests, graphical user interface web application penetration tests, web services application penetration tests, and wireless network penetration tests. Writes and reviews formal penetration test reports documenting the details of a penetration test and vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Works with Security Architects and Security Engineers to gather information and conduct penetration tests. Reviews and processes static source code vulnerability analysis reports for developed applications as directed. Supports evaluation of commercial and open source tools to be used for the purposes of penetration testing. Maintains demonstrable knowledge of current vulnerability exploitation techniques. Strong understanding of TCP/IP. Mentors junior Penetration Testers as needed. Researches new vulnerabilities and exploits in technologies directly relevant to the client/program.

**Experience:** 8 total experience with at least 4 years of related experience in information technology and/or information security. Certifications (at least one cert preferred)  
Certified Ethical Hacker (CEH) or equivalent certification  
Certified Penetration Tester (CPT) or equivalent certification  
Offensive Security Certified Expert (OSCE) or equivalent certification  
Offensive Security Exploitation Expert (OSEE) or equivalent certification  
Offensive Security Web Expert (OSWE) or equivalent certification  
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification  
eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) or equivalent certification

7. **Penetration Testing - Manager/Lead**  
**Education:** Bachelor's Degree

As the lead Tester conducts internal and external network penetration tests, graphical user interface web application penetration tests, web services application penetration tests, and wireless network penetration tests. Responsible for writing and reviewing formal penetration test reports documenting the details of a penetration test and all vulnerabilities, potential issues, and strengths found during the test. Responsible for submitting tickets for remediation of vulnerabilities and potential issues found during penetration tests. Works with Security Architects and Security Engineers to gather information and conduct penetration tests. Reviews and processes static source code vulnerability analysis reports for developed applications as directed. Leads the evaluation of commercial and open source tools to be used for the purposes of penetration testing. Maintains demonstrable knowledge of current vulnerability exploitation techniques. Strong understanding of TCP/IP. Mentors junior Penetration Testers as needed. Researches new vulnerabilities and exploits in technologies directly relevant to the client/program.

**Experience:** 8 total experience with at least 4 years of related experience in information technology and/or information security. Certifications (at least one cert preferred)  
Certified Ethical Hacker (CEH) or equivalent certification  
Certified Penetration Tester (CPT) or equivalent certification  
Offensive Security Certified Expert (OSCE) or equivalent certification  
Offensive Security Exploitation Expert (OSEE) or equivalent certification  
Offensive Security Web Expert (OSWE) or equivalent certification  
GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certification  
eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX) or equivalent certification

8. **Incident Response Team – Principal**  
**Education:** Bachelor's Degree
Provides consulting and executive support to enterprise-wide or national level programs and personnel. Provides executive knowledge and insight, technical experience and/or subject-matter expertise to projects. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Performs enterprise-wide strategic systems planning.

Experience: 12 years of experience supporting the resolution of extremely complex systems engineering, computer science, or other related issues or provides in-depth domain expertise.

9. Incident Response Team – Subject Matter Expert (SME)
Education: Bachelor’s Degree in Information Systems Engineering, Computer Science, Engineering, Business or other related field

Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: 10 years of experience with 8 years of information systems management experience. Certifications (at least one cert preferred): GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Reverse Engineering Malware (GREM), EnCE or similar

10. Incident Detection/Response Analyst II
Education: Associate’s Degree

Performs hunting activities to search the network for indicators of compromise. Provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Performs live response data collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files. Performs incident response and malware analysis to investigate incidents and potential indicators of compromise. Helps determine the extent of the compromise, attributes of any malware and possible data exfiltrated. Researches and incorporates relevant threat intelligence during the investigation and in written and verbal reports.

Experience: 2 years direct subject matter experience and a total of 6 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN). Certifications (at least one cert preferred): GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Reverse Engineering Malware (GREM), EnCE or similar

11. Incident Detection/Response Analyst III
Education: Associate’s Degree

Performs hunting activities to search the network for indicators of compromise. Provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Performs live response data collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files. Performs incident response and malware analysis to investigate incidents and potential indicators of compromise. Determines the extent of the compromise, attributes of any malware and possible data exfiltrated. Researches and incorporates relevant threat intelligence during the investigation and in written and verbal reports. Develops, documents and manages containment strategy. Maintains current knowledge of tools and best-practices in advanced persistent threats; tools, techniques, and procedures of attackers; and forensics and incident response.

Experience: 4 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN). Certifications (at least one cert preferred) GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Reverse Engineering Malware (GREM), EnCE or similar
12. Incident Detection/Response Analyst IV

Education: Bachelor’s Degree

Performs hunting activities to search the network for indicators of compromise. Provides immediate onsite services to the customer in the event of the identification of a compromise or a credible alert from an intrusion detection system. Performs live response data collection and analysis on hosts of interest in an investigation. Correlates and analyze relevant events from host and network device log files. Performs incident response and malware analysis to investigate incidents and potential indicators of compromise. Determines the extent of the compromise, attributes of any malware and possible data exfiltrated. Researches and incorporates relevant threat intelligence during the investigation and in written and verbal reports. Develops, documents and manages containment strategy. Maintains current knowledge of tools and best-practices in advanced persistent threats; tools, techniques, and procedures of attackers; and forensics and incident response.

Experience: 2 year’s direct subject matter experience and a total of 6 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN). Certifications (at least one cert preferred): GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Reverse Engineering Malware (GREM), EnCE or similar

13. Incident Detection/Response Manager - Lead

Education: Bachelor’s Degree

Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: 4 year’s direct subject matter experience and a total of 8 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN). Certifications (at least one cert preferred): GIAC Certified Incident Handler (GCIH), GIAC Certified Forensic Analyst (GCFA), GIAC Reverse Engineering Malware (GREM), EnCE or similar


Education: Associate’s Degree

Under direct supervision, performs network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors Security Information and Event Management (SIEM) to identify security issues for remediation. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information.

Experience: 1 year of related experience in information technology and/or information security preferred Certifications (Desirable): CompTIA Security+, SANS GSEC, GCIH, GCIA, Carnegie Mellon SEI Certified Incident Handler. Security. EC Council C|EH, Microsoft MCSE

15. Security Operations Center (SOC) Analyst II

Education: Associate’s Degree

Performs network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors Security Information and Event Management (SIEM) to identify security issues for remediation. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Communicates alerts to agencies regarding intrusions and compromises to their...
network infrastructure, applications and operating systems. Assists with implementation of counter-measures or mitigating controls. Supports efforts to consolidate and conduct comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks. Supports Team Lead on developing recommendations for changes to Standard Operating Procedures and other similar documentation.

Experience: 2 years of related experience in information technology and/or information security preferred

16. Security Operations Center (SOC) Analyst III
Education: Associate’s Degree

Performs network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors and analyzes Security Information and Event Management (SIEM) to identify security issues for remediation. Knowledge of creating Security Information Event Management (SIEM) tool rules. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Communicates alerts to agencies regarding intrusions and compromises to their network infrastructure, applications and operating systems. Assists with implementation of counter-measures or mitigating controls. Supports efforts to consolidate and conduct comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks. Supports Team Lead on developing recommendations for changes to Standard Operating Procedures and other similar documentation.

Experience: 4 years of related experience in information technology and/or information security preferred.
Certifications (at least one cert preferred): CompTIA Security+, SANs GSEC, GCIH, GCIA. Carnegie Mellon SEI Certified Incident Handler. Security. EC Council C|EH, Microsoft MCSE

17. Security Operations Center (SOC) Analyst IV
Education: Associate’s Degree

Performs network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies. Monitors and analyzes Security Information and Event Management (SIEM) to identify security issues for remediation. Knowledge of creating Security Information Event Management (SIEM) tool rules. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Communicates alerts to agencies regarding intrusions and compromises to their network infrastructure, applications and operating systems. Implements counter-measures or mitigating controls. Consolidates and conducts comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks. Recommends changes to Standard Operating Procedures and other similar documentation. Generates end-of-shift reports for documentation and knowledge transfer to subsequent analysts on duty. May lead small groups on non-complex efforts.

Experience: 6 year’s direct experience with a total of 4 years of related experience in information technology and/or information security preferred Certifications (at least one cert preferred) CompTIA Security+, SANs GSEC, GCIH, GCIA, Carnegie Mellon SEI Certified Incident Handler. Security. EC Council C|EH, Microsoft MCSE

18. Security Operations Center (SOC) – Manager/Lead
Education: Associate’s Degree

Leads a team and/or project in performing network security monitoring and incident response for a large organization, coordinates with other government agencies to record and report incidents. Maintains records of security monitoring and incident response activities, utilizing case management and ticketing technologies.
Monitors and analyzes Security Information and Event Management (SIEM) to identify security issues for remediation. Knowledge of creating Security Information Event Management (SIEM) tool rules. Recognizes potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information. Communicates alerts to agencies regarding intrusions and compromises to their network infrastructure, applications and operating systems. Implements countermeasures or mitigating controls. Consolidates and conducts comprehensive analysis of threat data obtained from classified, proprietary, and open source resources to provide indication and warnings of impending attacks against unclassified and classified networks. Recommend changes to Standard Operating Procedures and other similar documentation. Generates end-of-shift reports for documentation and knowledge transfer to subsequent analysts on duty. Prepares reports and monitors performance of subordinates.

Experience: 8 year’s direct experience with a total of 8 years of related experience in information technology and/or information security preferred Certifications (at least one cert preferred) CompTIA Security+, SANs GSEC, GCIA, GCIA. Carnegie Mellon SEI Certified Incident Handler. Security. EC Council C|EH, Microsoft MCSE

19. Cyber Hunt Team - Principal
Education: Bachelor’s Degree

Provides consulting and executive support to enterprise-wide or national level programs and personnel. Provides executive knowledge and insight, technical experience and/or subject-matter expertise to projects. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Performs enterprise-wide strategic systems planning.

Experience: 12 years of experience supporting the resolution of extremely complex systems engineering, computer science, or other related issues or provides in-depth domain expertise.

20. Cyber Hunt Team - Subject Matter Expert (SME)
Education: Bachelor’s Degree

Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: 10 years of experience with 8 years of information systems management experience. Certifications (must have at least 1 of the following as appropriate), PMP, ITIL, Network or OS technology: MCSE; CCNA; etc. Information Security: GCIA; GCIH; CEH; CISSP; CISM; SSCP

21. Malware Detection Analyst II
Education: Associate’s Degree

Works closely with other security team members. Help design software to protect both hardware and software assets. Protect from outside cyber threats as well as any malware that could send data from the internal network to a hacker’s server. Malware analyst responsibilities normally revolve around software threats, can be a part of network security teams to bring overall support for enterprise networks. Responsibilities include: document malware threats and identify procedures to avoid them, analyze programs and software using analysis programs to identify threats and classify malware based on threats and commonalities.

Experience: 2 years of related experience, Certification (desired) in one or more of the following: CompTIA Network+, CPT: Certified Penetration Tester, CEPT: Certified Expert Penetration Tester, CREA: Certified Reverse Engineering Analyst, CEH: Certified Ethical Hacker, CWAPT: Certified Web Application Penetration Tester

22. Malware Detection Analyst III
Education: Associate's Degree
Works closely with other security team members, such as security analysts, architects, and administrators. Assist design software to protect both hardware and software assets. Protect from outside cyber threats as well as any malware that could send data from the internal network to a hacker’s server. Malware analyst responsibilities normally revolve around software threats, sometimes are a part of network security teams to bring overall support for enterprise networks. Responsibilities include: document malware threats and identify procedures to avoid them, analyze programs and software using analysis programs to identify threats and classify malware based on threats and commonalities, keep up-to-date on the latest malware threats and keep software updated to defend against them and write alerts to let security personnel know about the latest threats. Also help create documentation for corporate security policies.

Experience: 4 years of related experience, Certification (desired) in one or more of the following: CompTIA Network+, CPT: Certified Penetration Tester, CEPT: Certified Expert Penetration Tester, CREA: Certified Reverse Engineering Analyst, CEH: Certified Ethical Hacker, CWAPT: Certified Web Application Penetration Tester

### 23. Malware Detection Analyst IV

**Education:** Associate's Degree

Works closely with other security team members, such as security analysts, architects, and administrators. Assist design software to protect both hardware and software assets. Protect from outside cyber threats as well as any malware that could send data from the internal network to a hacker’s server. Malware analyst responsibilities that revolve around software threats, sometimes are a part of network security teams to bring overall support for enterprise networks. Responsibilities include: document malware threats and identify procedures to avoid them, analyze programs and software using analysis programs to identify threats and classify malware based on threats and commonalities, keep up-to-date on the latest malware threats and keep software updated to defend against them and write alerts to let security personnel know about the latest threats. Also help create documentation for corporate security policies and may support training personnel and other team members on best security practices.

Experience: 6 years of related experience, Certification (desired) in one or more of the following: CompTIA Network+, CPT: Certified Penetration Tester, CEPT: Certified Expert Penetration Tester, CREA: Certified Reverse Engineering Analyst, CEH: Certified Ethical Hacker, CWAPT: Certified Web Application Penetration Tester

### 24. Malware Detection – Manager/Lead

**Education:** Bachelor's Degree

Working as the team lead, works closely with other security team members, including security analysts, architects, and administrators. Support efforts for software design to protect both hardware and software assets. Protect from outside cyber threats as well as any malware that could send data from the internal network to a hacker’s server. Responsibilities revolve around software threats, but they can sometimes be a part of network security teams to bring overall support for enterprise networks. Responsibilities include: document malware threats and identify procedures to avoid them, analyze programs and software using analysis programs to identify threats and classify malware based on threats and commonalities, keep up-to-date on the latest malware threats and keep software updated to defend against them and write alerts to let security personnel know about the latest threats. Oversee creation of documentation for corporate security policies and may support training personnel and other team members on best security practices. And understands tools that identify zero-day cyber threats and work to protect from them and participate in research and development of malware protection tools.

Experience: 8 years of related experience, Certification (desired) in one or more of the following: CompTIA Network+, CPT: Certified Penetration Tester, CEPT: Certified Expert Penetration Tester, CREA: Certified Reverse Engineering Analyst, CEH: Certified Ethical Hacker, CWAPT: Certified Web Application Penetration Tester

### 25. Threat Intelligence Analyst I

**Education:** Associate's Degree
Collects intelligence including Indicators of Compromise (IOCs). Develops and maintains specialized knowledge related to crime ware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and DDOS techniques. Maintains security systems log files, reconciles correlated security events, and further develops current security event correlation capabilities. Supports investigations with intelligence collection, analysis, and/or dissemination. Conducts independent research to identify cybersecurity threats; and produces analytical products. Compiles and analyzes cyber threat information and making recommendations based on suspected or known context to draw insights and conclusions regarding its relative threats. Produces; edits; and distributes a variety of concise and actionable threat analysis and warning products in electronic and/or written and presentation form to stakeholders/customers. Supports studies to identify cyber threats; threat vectors; threat actors; and threat trends. Identifies threat signatures from available sources. Supports standard procedures for incident response. Interfaces with Security Officers and Incident Response Teams. Desirable to have working knowledge of technical security countermeasures systems and regulations regarding technical, physical, and procedural security.

Experience: 6 months of related experience, Certification (desirable)
Network or OS technology: MCSE; CCNA; etc.
Information Security: GCIA; GCIH; CEH; CISSP; CISM; SSCP

26. Threat Intelligence Analyst II
Education: Associate's Degree

Collects intelligence including Indicators of Compromise (IOCs). Develops and maintains specialized knowledge related to crime ware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and DDOS techniques. Maintains and analyzes security systems log files, reconciles correlated security events, and further develops current security event correlation capabilities. Supports investigations with intelligence collection, analysis, and/or dissemination. Conducts independent research to identify cybersecurity threats; and produces analytical products. Compiles and analyzes cyber threat information and making recommendations based on suspected or known context to draw insights and conclusions regarding its relative threats. Produces; edits; and distributes a variety of concise and actionable threat analysis and warning products in electronic and/or written and presentation form to stakeholders/customers. Conducts studies and makes recommendations to identify cyber threats; threat vectors; threat actors; and threat trends. Identifies and develops threat signatures from available sources. Maintains threat indicators in a threat intelligence platform. Implements and supports standard procedures for incident response. Interfaces with Security Officers and Incident Response Teams. Has knowledge and understanding of intelligence community standards and directives. Desirable to have working knowledge of technical security countermeasures systems and regulations regarding technical, physical, and procedural security.

Experience: 2 years of related experience, Certification (desirable): Network or OS technology: MCSE; CCNA; etc., Information Security: GCIA; GCIH; CEH; CISSP; CISM; SSCP

27. Threat Intelligence Analyst – Manager/Lead
Education: Bachelor's Degree

Leads teams and/or Projects for collecting intelligence including Indicators of Compromise (IOCs). Develops and maintains specialized knowledge related to crime ware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and DDOS techniques. Maintains and analyzes security systems log files, reconciles correlated security events, and further develops current security event correlation capabilities. Performs investigations with intelligence collection, analysis, and/or dissemination. Conducts independent research to identify cybersecurity threats; and produces analytical products. Compiles and analyzes cyber threat information and making recommendations based on suspected or known context to draw insights and conclusions regarding its relative threats. Produces; edits; and distributes a variety of concise and actionable threat analysis and warning products in electronic and/or written and presentation form to stakeholders/customers. Conducts studies and makes recommendations to identify cyber threats; threat vectors; threat actors; and threat trends. Identifies and develops threat signatures from available sources. Maintains threat indicators in a threat intelligence platform. Implements and supports standard procedures for incident response. Interfaces with Security Officers and Incident Response Teams. Represents team internal and external threat intelligence and cybersecurity forums. Has knowledge and understanding of
intelligence community standards and directives. Desirable to have working knowledge of technical security countermeasures systems and regulations regarding technical, physical, and procedural security. Communicates with stakeholders and other team/project leaders.

Experience: 6 years of related experience, Certification (at least one): Network or OS technology: MCSE; CCNA; etc., Information Security: GCIA; GCIH; CEH; CISSP; CISM; SSCP

28. Risk and Vulnerability Assessment Team – Principal
Education: Bachelor's Degree

Provides consulting and executive support to enterprise-wide or national level programs and personnel. Provides executive knowledge and insight, technical experience and/or subject-matter expertise to projects. Performs analyses and develops recommendations that may have substantial impact on major programs and activities. Performs enterprise-wide strategic systems planning.

Experience: 12 years of experience supporting the resolution of extremely complex systems engineering, computer science, or other related issues or provides in-depth domain expertise.

29. Risk and Vulnerability Assessment Team – Subject Matter Expert (SME)
Education: Bachelor's Degree

Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: 10 years of experience with 8 years of information systems management experience. Certifications (must have at least 1 of the following as appropriate): PMP, ITIL, CISA, CISSP, CISM, SCP

30. Security Controls Assessment Analyst I
Education: Bachelor's Degree

Supports efforts to define and document a detailed suite of controls to meet the client/program control objectives/directives. May provide ancillary support in the development and implementation of a Risk Governance Framework. Supports documenting Control Requirements considering regulatory requirements, authoritative control frameworks and industry best practices. Works under the direction of Control Owners and Security Architects across various technology platforms and organizations. Documents Control Operating Procedures as required. Supports efforts to document Control Testing Procedures and support them as needed in the development of remediation plans to address control issues. Supports the development and implementation of Security Controls Training & Awareness Program(s).

Experience: 6 months in IT operations, technology or operational risk management. Certifications (desirable): CISA, CISSP, CISM, SCP

31. Security Controls Assessment Analyst II
Education: Bachelor's Degree

Supports efforts to define and document a detailed suite of controls to meet the client/program control objectives/directives. May provide ancillary support in the development and implementation of a Risk Governance Framework. Supports documenting Control Requirements considering regulatory requirements, authoritative control frameworks and industry best practices. Works under the direction of Control Owners and Security Architects across various technology platforms and organizations. Documents Control Operating Procedures as required. Supports efforts to document Control Testing Procedures and support them as needed in the development of remediation plans to address control issues. Supports the development and
implementation of Security Controls Training & Awareness Program(s). Assists with the development of Control Strategy & Road mapping addressing maturing systems.

Experience: 2 years in IT operations, technology or operational risk management.
Certifications (at least one preferred): CISA, CISSP, CISM. SCP

32. **Security Controls Assessment Analyst IV**

Education: Bachelor's Degree

Serves as the authorized interface with the client on large or complex information technology programs. Performs program management and oversight to ensure successful program performance. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor and subcontractor personnel, and communicating policies, purposes, and goals of the organization to subordinates. May perform enterprise-wide horizontal integration planning and interfaces with other functional systems. Responsible for overall contract performance.

Experience: 2 years in IT operations, technology or operational risk management.
Certifications (at least one preferred): CISA, CISSP, CISM. SCP

33. **Information Assurance Engineer I**

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Responsible for supporting Information Assurance engineering teams with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Required basic understanding of approved COTS security analyst tools and government mitigation/ compliance checkers. Basic comprehension of FISMA, DIACAP, NIST, ISO and DCID standards and policy control grouping. Assist in determining products to meet needs and presents results. Supports system performance and maintaining system security, as well as troubleshooting any system security problems. May be responsible for both local and remote administration of networks.

Experience: Must have at least 2 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN).
Certifications: MCP, CompTIA-Network +, CompTIA-Security +

34. **Information Assurance Engineer II**

Education: Bachelor's Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Responsible for technical information assurance engineering efforts with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Experience in ST&E process and POAM generation. Requires strong understanding of approved COTS security analyst tools and government mitigation/compliance checkers. Strong comprehension of FISMA, DIACAP, NIST, ISO and DCID standards and policy control grouping. Experience determining products to meet client needs and presenting results. Acts a tier two support engineer during system performance testing. Experience providing tier two support and troubleshooting any system security problems arising from security lockdowns. May be responsible for both local and remote administration of networks.

Experience: Must have 8 years of experience with at least 3 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN) and 3 years of security engineering, system security auditing or system penetration testing.
Certifications: MCSA/Unix/Linux, CCNA, CompTIA-Network +, CompTIA-Security +, CISSP

35. **Information Assurance Engineer III**

Education: Bachelor’s Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.
Responsible for technical information assurance engineering efforts with network/server scanning, patching, mitigation, and compliance cross-checking of target network assets. Experience in ST&E process and POAM generation. Requires strong understanding of approved COTS security analyst tools and government mitigation/compliance checkers. Strong familiarity with FISMA, DIACAP, NIST, ISO and DCID, OMB Circulars. Experience determining products to meet client needs and presenting results. Acts a tier three support engineer during system performance testing. Experience providing tier three support & troubleshooting any system security problems arising from security lockdowns. May be responsible for minor customer interface and IA site engineering leadership.

Experience: Must have 10 years of experience with at least 4 years of technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN) and 4 years of security engineering, system security auditing or system penetration testing. 

Certifications: MCSE/Unix/Linux, CCNA/CCNP CompTIA-Network+, CompTIA-Security+, CISSP

36. Information Assurance Policy Analyst

Education: Bachelor’s Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Provide Information Assurance support in tracking, reporting and providing guidance in FISMA, DIACAP, NIST, ISO and DCID standards and policy control grouping. Manage and track annual security compliance activities including but not limited to incident response testing, contingency testing, and policy and procedures. Provide updates to Administration of Access Control Program, manage access/ account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Enforcement and re-alignment of security policy with the document change management process Plan of Action and Milestones (POAM), manage and track completion dates for POAM items, assemble remediation packages for POAM items and perform remediation of findings involving security program compliance.

Experience: Must have 6 years of experience with at least 4 years of Information Assurance Policy experience in security administration, evaluation of security/Information Assurance product capabilities, assessment and policy development. 

Certifications: CompTIA-Network +, CompTIA-Security +, CISSP

37. Senior Information Assurance Policy Analyst

Education: Bachelor’s Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.

Provide Information Assurance expertise in tracking, reporting and providing guidance in FISMA, DIACAP, NIST, ISO and DCID standards and policy control grouping. Manage and track annual security compliance activities including but not limited to incident response testing, contingency testing, and policy and procedures. Provide updates to Administration of Access Control Program, manage access/ account control process including collecting, distributing, tracking and storing access request forms, perform annual user revalidation documentation updates. Prepare certification analysis and reports, develop or review certification test plans, and provide certification recommendations. Enforcement and re-alignment of security policy with the document change management process Plan of Action and Milestones (POAM), manage and track completion dates for POAM items, assemble remediation packages for POAM items and perform remediation of findings involving security program compliance. Develop a security concept of operations from user requirements or source documents that addresses all of the user’s functional and security requirements.

Experience: Must have 10 years of experience with at least 7 years of Information Assurance Policy experience in security administration, evaluation of security/Information Assurance product capabilities, assessment and policy development. 

Certifications: CompTIA-Network +, CompTIA-Security +, CISSP

38. Information Assurance Subject Matter Expert (SME)

Education: Master’s Degree in Information Systems, Security, Engineering, or other related scientific or technical discipline.
Provide Information Assurance expertise in tracking, reporting and providing guidance in FISMA, DIACAP, NIST, ISO and DCID standards and policy control grouping. Provide senior guidance on the development of and acceptance by civilian and defense Government agencies on Information Assurance plans; system evolution; capabilities; compliance with FISMA, DIACAP, DCID, NIST, FIPS, and legal or statutory requirements. Serve as advisor to CIO, CTO, CISO, Program Director, Systems Owner, or Operations Managers to develop, implement, and manage Information Assurance as a core competence. Must have extensive experience in design, test, evaluation, certification and accreditation of systems. Must also possess strong background in Cross Domain Solutions and cross contamination avoidance methodologies. Core skill in requirements analysis, requirements writing, development of security architectures, secure network protocols, secure authentication technologies, intrusion detection systems, information assurance standards and policies, and forensic analysis.

Experience: Must have 15 years of experience with at least 10 years of Information Assurance Policy; technical experience installing, maintaining, and managing Local Area Networks (LANs) or Wide Area Networks (WAN); or security engineering, system security auditing, or system penetration testing.

Certifications: MCSA/MCSE, CCNA/CCNP, CompTIA-Network +, CompTIA-Security +, CISSP

39. Vulnerability Management Analyst I

Education: Associate’s Degree

Protects against unauthorized access, modification, or destruction. Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization. Implements, upgrades, or monitors security measures for the protection of computer networks and information. Documents potential incidents and initiation of response teams. Identifies security risks and develop solutions to eliminate or minimize risks. Vulnerability management and remediation using various tools and systems. Supports oversight of security environments. Good working knowledge of cyber security methodology and security practices. Experience with threat assessment, vulnerability analysis, risk assessment, information gathering, correlating and reporting. Experience with current packet capture and event aggregation tools. Support mitigations for vulnerabilities, exploits, patches. Ability to read network logs and analyze network packet capture data. Train end users and promote security awareness to ensure system security and to improve server and network efficiency.

Experience: 1-year Information Technology related experience with a minimum of 6 months Information Security related experience. Certification (desirable): Global Information Assurance Certificate (GIAC) Certified Incident Handler (GCIH) certification, CISSP, CISM, CRISC or similar certification

40. Vulnerability Management Analyst II

Education: Associate’s Degree

Maintains Information Security documentation storage, attestations and version updates. Tracks compliance-based initiatives to completion and generates workflows to streamline processes. Works closely with compliance team members to aid in regulatory tracking and compliance. Protects against unauthorized access, modification, or destruction. Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization. Implements, upgrades, or monitors security measures for the protection of computer networks and information. Documents potential incidents and initiation of response teams. Identifies security risks and develop solutions to eliminate or minimize risks. Vulnerability management and remediation using various tools and systems. Supports oversight of security environments. Good working knowledge of cyber security methodology and security practices. Experience with threat assessment, vulnerability analysis, risk assessment, information gathering, correlating and reporting. Experience with current packet capture and event aggregation tools. Support mitigations for vulnerabilities, exploits, patches. Ability to read network logs and analyze network packet capture data. Train end users and promote security awareness to ensure system security and to improve server and network efficiency.
Experience: 2 years Information Technology related experience. Certification (desirable): Global Information Assurance Certificate (GIAC) Certified Incident Handler (GCIH) certification, CISSP, CISM, CRISC or similar certification

41. Vulnerability Management Analyst III
Education: Bachelor's Degree

Data Loss Prevention -- Develops plans to safeguard sensitive information in motion and at rest for both digital and non-digital against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs. Maintains Information Security documentation storage, attestations and version updates. Tracks compliance-based initiatives to completion and generates workflows to streamline processes. Works closely with compliance team members to aid in regulatory tracking and compliance. Protects against unauthorized access, modification, or destruction. Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization. Implements, upgrades, or monitors security measures for the protection of computer networks and information. Documents potential incidents and initiation of response teams. Identifies security risks and develop solutions to eliminate or minimize risks. Vulnerability management and remediation using various tools and systems. Supports oversight of security environments. Good working knowledge of cyber security methodology and security practices. Experience with threat assessment, vulnerability analysis, risk assessment, information gathering, correlating and reporting. Experience with current packet capture and event aggregation tools. Support mitigations for vulnerabilities, exploits, patches. Ability to read network logs and analyze network packet capture data. May Train end users and promote security awareness to ensure system security and to improve server and network efficiency.

Experience: 2 years Information Technology related experience with a minimum of 6 months Information Security related experience. Certification (desirable): Global Information Assurance Certificate (GIAC) Certified Incident Handler (GCIH) certification, CISSP, CISM, CRISC or similar certification

42. Vulnerability Management Analyst IV
Education: Bachelor's Degree

Collaborates with users to discuss issues such as computer data access needs, security violations, and development challenges. Monitors current reports of computer viruses to determine when to update virus protection systems. Data Loss Prevention -- Develops plans to safeguard sensitive information in motion and at rest for both digital and non-digital against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs. Maintains Information Security documentation storage, attestations and version updates. Tracks compliance-based initiatives to completion and generates workflows to streamline processes. Works closely with compliance team members to aid in regulatory tracking and compliance. Protects against unauthorized access, modification, or destruction. Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization. Implements, upgrades, or monitors security measures for the protection of computer networks and information. Documents potential incidents and initiation of response teams. Identifies security risks and develop solutions to eliminate or minimize risks. Vulnerability management and remediation using various tools and systems. Supports oversight of security environments. Good working knowledge of cyber security methodology and security practices. Experience with threat assessment, vulnerability analysis, risk assessment, information gathering, correlating and reporting. Experience with current packet capture and event aggregation tools. Support mitigations for vulnerabilities, exploits, patches. Ability to read network logs and analyze network packet capture data. May develop Information Security Metrics program. May Train end users and promote security awareness to ensure system security and to improve server and network efficiency. Mentors junior Vulnerability Management Analysts.

Experience: 4 years Information Technology related experience with a minimum of 2 years Information Security related experience. Certification (at least one): Global Information Assurance Certificate (GIAC) Certified Incident Handler (GCIH) certification, CISSP, CISM, CRISC or similar certification
43. Vulnerability Management Analyst – Manager/Lead

Education: Bachelor’s Degree

Leads Team in all Vulnerability Management efforts. Collaborates with users to discuss issues such as computer data access needs, security violations, and development challenges. Monitors current reports of computer viruses to determine when to update virus protection systems. Data Loss Prevention -- Develops plans to safeguard sensitive information in motion and at rest for both digital and non-digital against accidental or unauthorized modification, destruction, or disclosure and to meet emergency data processing needs. Maintains Information Security documentation storage, attestations and version updates. Tracks compliance-based initiatives to completion and generates workflows to streamline processes. Works closely with compliance team members to aid in regulatory tracking and compliance. Protects against unauthorized access, modification, or destruction. Works with end users to determine needs of individual departments, implements policies or procedures, and tracks compliance through the organization. Implements, upgrades, or monitors security measures for the protection of computer networks and information. Documents potential incidents and initiation of response teams. Identifies security risks and develop solutions to eliminate or minimize risks. Vulnerability management and remediation using various tools and systems. Supports oversight of security environments. Good working knowledge of cyber security methodology and security practices. Experience with threat assessment, vulnerability analysis, risk assessment, information gathering, correlating and reporting. Experience with current packet capture and event aggregation tools. Support mitigations for vulnerabilities, exploits, patches. Ability to read network logs and analyze network packet capture data. May train end users and promote security awareness to ensure system security and to improve server and network efficiency. Mentors and directs Vulnerability Management Analysts.

Experience: 6 years Information Technology related experience with a minimum of 4 years Information Security related experience. Certification (at least one): Global Information Assurance Certificate (GIAC) Certified Incident Handler (GCIH) certification, CISSP, CISM, CRISC or similar certification
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

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

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

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

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

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

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

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

Jacobs Technology Inc.
600 William Northern Blvd.
Tullahoma, TN 37388-4729
Office: (703) 896-4000 Fax: (703) 435-9715
www.jacobstechnology.com
Point of Contact: Rhonda Pari, Rhonda.pari@jacobs.com
BLANKET PURCHASE AGREEMENT I - FEDERAL SUPPLY SCHEDULE

CUSTOMER NAME  
(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act

(Ordering activity)

And

(Contractor)

enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) ______.

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

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

Signatures

______________________________________________________________________________  
Ordering Activity  
Date

______________________________________________________________________________  
Contractor  
Date
BLANKET PURCHASE AGREEMENT II

(CUSTOMER NAME)

BPA NUMBER: __________________________

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

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

| MODEL NUMBER/PART NUMBER | *SPECIAL BPA DISCOUNT/PRICE |

(2) Delivery:

| DESTINATION | DELIVERY SCHEDULES / DATES |

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

(4) This BPA does not obligate any funds.

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

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

| OFFICE | POINT OF CONTACT |

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

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

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

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

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

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

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

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

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

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

Here is a general outline on how it works:

The customer identifies their requirements.

- Federal Supply Schedule Contractors may individually meet the customer’s needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.