GSA Advantage!
Multiple Award Schedule

Service Catalog Information
Table of Contents

COMPANY INFORMATION........................................................................................................ 3
CONTRACT INFORMATION...................................................................................................... 4
CUSTOMER INFORMATION...................................................................................................... 6
LABOR DESCRIPTIONS (54151S)............................................................................................ 13
LABOR DESCRIPTIONS (54151HACS) ................................................................................... 67
  High Value Asset Assessments.......................................................................................... 67
  Risk and Vulnerability Assessment.................................................................................. 72
  Cyber Hunt....................................................................................................................... 74
  Incident Response ............................................................................................................ 75
  Penetration Testing........................................................................................................... 77
PRICE LIST TO GSA.............................................................................................................. 79
## COMPANY INFORMATION

<table>
<thead>
<tr>
<th>Name</th>
<th>Web Traits, Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>9423 Eagleton Lane</td>
</tr>
<tr>
<td></td>
<td>Montgomery Village, MD 20886</td>
</tr>
<tr>
<td>Phone</td>
<td>(240)731-6120</td>
</tr>
<tr>
<td>Fax</td>
<td>(240)553-1295</td>
</tr>
<tr>
<td>Web Address</td>
<td><a href="http://web-traits.com/">http://web-traits.com/</a></td>
</tr>
<tr>
<td>Point of Contact</td>
<td>Bhaskar Roy</td>
</tr>
<tr>
<td><strong>CONTRACT INFORMATION</strong></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Contract Number</strong></td>
<td>GS-35F-134AA</td>
</tr>
<tr>
<td><strong>Schedule Description</strong></td>
<td>Multiple Award Schedule – Large Category F – Information Technology</td>
</tr>
<tr>
<td><strong>SIN Number</strong></td>
<td>54151S and 54151HACS</td>
</tr>
</tbody>
</table>
| **SIN Description**      | 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES  
                          | 54151HACS - HIGHLY ADAPTIVE CYBERSECURITY SERVICES |
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE

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

SCHEDULE TITLE: MULTIPLE AWARD SCHEDULE
FCS GROUP: INFORMATION TECHNOLOGY
SPECIAL ITEM NUMBER: 54151S - Information Technology (IT) Professional Services
54151HACS – Highly Adaptive Cybersecurity Services
FSC/PSC CODE: D399

Web Traits, Inc.
9423 Eagleton Ln / Montgomery Village, MD 20886-1242
Telephone Number: (240) 731-6120
www.web-traits.com

Contract Number: GS-35F-134AA
Price List Effective Date: Effective through Modification No. PS-0022 effective 9.10.20
Period Covered by Contract: December 20, 2017 through December 20, 2022
Business Size: Small Business
SBA Certified Small Disadvantaged Business

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov.
CUSTOMER INFORMATION

1. Awarded Special Item Number(s):

<table>
<thead>
<tr>
<th>SIN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S, 54151SRC</td>
<td>IT Professional Services</td>
</tr>
<tr>
<td>54151HACS, 54151HACSRC</td>
<td>Highly Adaptive Cybersecurity Services</td>
</tr>
</tbody>
</table>

1b. Identification of the lowest priced labor category description and hourly rate awarded under the contract is:

<table>
<thead>
<tr>
<th>Labor Category Description</th>
<th>GSA Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Administrator I</td>
<td>$63.53</td>
</tr>
</tbody>
</table>

Responsibilities

- Maintain system documentation and logs
- Perform systems administration functions for the District wide e-mail system
- Maintain application security, event investigations and compliance enforcement.
- Administer secure links with public key encryption, anti-virus, user authentication and intrusion detection
- Provide monitoring and primary response and intervention for information technology related security incidents and violations
- Keep current with new Information Technology Security protocols, applicable laws and regulations
- Management of Active Directory
- Management of users and computers
- Management of access to resources, computer environment etc.
- Monitoring network access
- Thorough understanding of TCP/IP, different protocols and OSI Model
- Quickly arrange repair for hardware in occasion of hardware failure
- Implement the policies for the use of the computer system and network
- Setup security policies for users. A system admin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems).

Experience

- Two years of increasingly responsible computer applications programming and systems analysis experience
- A minimum of two years progressive experience in various Information Technology related functions including but not limited to information server standard administration
- Strong operating system and network knowledge in order to carry out assigned administrative tasks with the need for limited supervision
- Overall system administration responsibility for major platform and operating systems
- Local Area Networks (LANs) and Wide Area Networks (WANs)
- Reporting tools, Excel, Crystal Reports, etc.

Education

- A bachelor’s degree from an accredited college or university with major course work in Computer Science, Management Information Systems, or a closely related field
1c. Labor Category Descriptions of all corresponding commercial job titles, experience, functional responsibility and education are outlined within this pricelist.

2. **Maximum Order:** $500,000

3. **Minimum Order:** $100

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

5. **Point of Production:** Montgomery Village, Maryland

6. **Discount from List:** Prices are net.

7. **Quantity Discount:** 2.5% Additional Discount for $6 mil and over per annual contract.

8. **Prompt Payment Terms:** 1% - 21 days from receipt of invoice or date of acceptance, whichever is later. Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9a. **Government Purchase Cards:** Government Purchase Cards will be accepted for payment on orders below the micro-purchase threshold. A 2% discount is offered on non-credit card payments.

9b. **Government Purchase Cards:** Government purchase cards are not accepted for payment on orders above the micro-purchase threshold.

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

11a. **Normal Delivery Terms:** As negotiated between Web Traits and the Ordering Activity.

11b. **Expedited Delivery Terms:** As negotiated between Web Traits and the Ordering Activity.

11c. **Overnight/2-Day Delivery Terms:** As negotiated between Web Traits and the Ordering Activity.

11d. **Urgent Requirements:** As negotiated between Web Traits and the Ordering Activity.

12. **FOB Point:** Destination

13a. **Ordering Address:** Web Traits, Inc. 9423 Eagleton Lane, Montgomery Village, MD 20886
13b. **Ordering Procedures:** For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA’s) are found in Federal Acquisition Regulation (FAR) 8.405-3.

14. **Payment Address:** Web Traits, Inc. 9423 Eagleton Lane, Montgomery Village, MD 20886

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

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

17. **Terms and Conditions of Government purchase card acceptance:** Web Traits does not accept payment by Government purchase card for amounts above the micro-purchase threshold.

18. **Terms and conditions of rental, maintenance, and repair (if applicable):** Not Applicable.

19. **Terms and conditions of installation (if applicable):** Not Applicable.

20. **Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable):** Not Applicable.

20a. **Terms and conditions for any other services (if applicable):** Not Applicable.

21. **List of service and distribute on points (if applicable):** Not Applicable.

22. **List of participating dealers (if applicable):** Not Applicable.

23. **Preventive maintenance (if applicable):** Not Applicable.

24a. **Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants):** None

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

25. **Data Universal Number System (DUNS) number:** Web Traits’ DUNS Number is 827402335.

26. **Notification regarding registration in System for Award Management (SAM) database:** Web Traits is registered in SAM.
1. **SCOPE**
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

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

   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.

   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity’s mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

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

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

4. **PERFORMANCE OF SERVICES**
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

   b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

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

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

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

   (1) Cancel the stop-work order; or

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

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

   (1) The stop-work order results in an increase in the time required for, or in the Contractor’s cost properly allocable to, the performance of any part of this contract; and

   (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

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

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

6. INSPECTION OF SERVICES

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

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. INDEPENDENT CONTRACTOR
All IT Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST
   a. Definitions.
   “Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
   “Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.
   An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.
   b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

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

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

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
   (1) The offeror;
   (2) Subcontractors; and/or
   (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

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

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

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING
A description of the labor categories offered and pricing begin on page 13 of this pricelist.
LABOR DESCRIPTIONS (54151S)

<table>
<thead>
<tr>
<th>1. Network Security Analyst I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Experience</strong></th>
<th>This position requires familiarity with:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Firewall rules</td>
</tr>
<tr>
<td></td>
<td>• Monitoring firewalls</td>
</tr>
<tr>
<td></td>
<td>• Managing security</td>
</tr>
<tr>
<td></td>
<td>• Incident reporting and resolution</td>
</tr>
<tr>
<td></td>
<td>• Capturing security events and data for reports generation</td>
</tr>
<tr>
<td></td>
<td>• Policy management of network firewalls</td>
</tr>
<tr>
<td></td>
<td>• Mitigating risks associated with firewall assets and their technical issues</td>
</tr>
<tr>
<td></td>
<td>• Maintaining trouble tickets and incident management</td>
</tr>
<tr>
<td></td>
<td>• Maintaining security log files</td>
</tr>
<tr>
<td></td>
<td>• Managing Firewall asset log and policy data</td>
</tr>
</tbody>
</table>

| **Education** | This position requires a minimum of a baccalaureate degree in related field with a minimum of 3+ years of work experience. Candidates with CCSA, CCSE, and CCMSE certifications will be given higher preference. CCNA or CCNP and ITIL certifications are highly desired. |
### 2. Network Security Analyst II

| Responsibilities                                                                 | In this role, the candidate provides and maintains authority-wide LAN/WAN computer hardware and software on a 24/7 basis. Typically, the candidate will collaborate with other Technical Support personnel to provide 24/7 coverage, as well as maintain WAN routers, switches, firewalls, and proxy servers. The job functions are:  
- Supporting communication links between facilities  
- Supporting communication links between Bridges and Tunnels, other office locations and the Internet  
- Interconnecting routers, hubs, servers, and PCs in a fast paced and diverse hardware and software environment  
- Providing immediate assistance and services to technicians and users  
- Responding to crisis  
- Responding, identifying, and resolving short-term issues  
- Developing and implementing a long-term proactive support system by providing guidance and assisting the hotline staff  
- Making decisions and determining issues that should be escalated  
- Following proper escalation procedures until issues are resolved  
- Informing the management and co-workers of the status of important issues  
- Defining & managing projects to meet project schedules  
- Meeting assignments milestones and deadlines |
| Experience                                                                         | This position requires 5+ years of specialized knowledge in:  
- Experience in troubleshooting switches, routers, frame-relay ATM and wireless  
- Experience in security event monitoring and intrusion detection/prevention  
- Commanding knowledge of TCP/IP protocol  
- Experience with network vulnerability assessment tools  
- Experience in policy and procedures development  
- Proficient in communication protocols, data and network security  
- In-depth knowledge of systems integration, client/server architecture, distributed processing, connectivity solutions etc.  
- Excellent system analysis techniques and analytical skills  
- Working knowledge of networking operating systems such as Novell Netware, Windows NT/2000, UNIX |
| Education                                                                         | This position requires a minimum of a baccalaureate degree from an accredited college or university or a high school diploma (or its educational equivalent) and seven years of work experience. Work experience must include:  
- 7 years of progressively more responsible, full-time, satisfactory experience using mainframe, PC, mini or micro-computer technologies in computer applications, programming, systems programming, computer systems development, data telecommunications, database administration and planning of data processing  
- At least 1.5 years of experience in an administrative, managerial, or executive capacity in the areas of computer applications programming, systems programming, computer systems development, data telecommunications, database administration and planning of data processing |
### 3. Network Security Analyst III

| **Responsibilities** | In this role, the candidate architects and designs solutions for the network and network-related components as well as provides secure solutions for the datacenter operation. The job functions are:  
- Interfacing with customers to understand their Security requirements  
- Assisting in designing security solutions for customers  
- Developing firewall rule change requests  
- Creating firewall scripts  
- Verifying proper configuration and operation of firewalls  
- Verify proper configuration and operation of security agents  
- Troubleshooting network connectivity issues  
- Assisting with firewall capacity management  
- Providing second tier technical support for firewalls and security tools for the Security Operations Center (SOC)  
- Evaluating and making recommendations for security products to enhance security posture of the datacenter  
- Evaluating and making recommendations for datacenter change requests to ensure they comply with security standards |

| **Experience** | This position requires 7+ years of knowledge of:  
- Popular networking components like CISCO Firewall, Firewall Services Module (FWSM), ASA 5580  
- Series Appliances etc.  
- VLAN/Trunking Protocol  
- CISCO Catalyst 6509 Series Switches, Symantec Security Endpoint Security (SEC) and Critical System Protection (CSP)  
- Designing and deploying systems like typical 3-tier architecture web front-end, application back-end and databases etc.  
- Expert-level understanding of 7-layers of OSI model  
- Expert-level understanding of TCP/IP ports and protocols  
- VMWare and VSphere |

| **Education** | This position requires a minimum of a baccalaureate degree in Computer Science or Information Systems from an accredited college or university or equivalent work experience. CISSP certification or equivalent is desired. |
### 4. Information Security Analyst I

**Responsibilities**

In this role, the candidate supports the development and implementation of IT Security controls that adhere to NIST guidelines. It supports the development and implementation policies and standards in regards to information systems and data within a datacenter. It ensures confidentiality, integrity and availability of all IT assets and data. This position requires:

- Ensuring the implementation, integrity and monitoring of security controls in accordance with the SSP and NIST policies and procedures
- Conducting and participating in annual security assessments
- Conducting and participating in security audits
- Providing security guidance to designated design and engineering personnel for service development
- Completing security controls verification for General Support System (GSS), Major or Minor Applications
- Completing security controls validation for General Support System (GSS), Major or Minor Applications
- Implementing policies, procedures and process reviews for General Support System (GSS), Major or Minor Applications
- Completing regular and periodic compliance/vulnerability scan assessments for General Support System (GSS), Major or Minor Applications

**Experience**

This position requires expert-level knowledge of:

- FIPS 199 Categorization
- FISMA Regulation
- NIST guidelines
- Privacy Impact Assessment
- e-Authentication
- System Security Plan (SSP)
- Security Test and Evaluation (ST&E) planning
- Risk Assessment (RA)
- Security Assessment Report (SAR)
- Authorization to Operate (ATO) Letter
- Plan of Action and Milestones (POA&M)
- Vulnerability Scan
- Self-Assessments reports

**Education**

This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 3+ years of work experience. An active CISSP certification is preferred.
### 5. Information Security Analyst II

**Responsibilities**

In this role, the candidate supports the development and implementation of IT Security Policies and Standards. It maintains confidentiality, integrity and availability of all IT assets and data. The job functions are:

- Providing timely reporting and escalation of security incidents
- Overseeing actions taken to resolve major security incidents
- Ensuring vendor provided security maintenance and patches are appropriately applied to IT assets and infrastructure
- Conducting regular and periodic audits and tests of IT security
- Providing regular and periodic Security reports to management

**Experience**

This position requires:

- Experience with special security investigations
- Managing SOC (Security Operations Center) activities
- Experience with recommending changes and improvements to support Security Management tools
- Ability to serve as a point of contact (POC) for all security matters related to the IT assets and systems
- Implementation and maintenance of security controls in accordance with the System Security Plan (SSP) and agency or corporate policies

**Education**

This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 5+ years of work experience. An active CISSP certification is preferred.

### 6. Information Security Analyst III (Cyber Security)

**Responsibilities**

In this role, the candidate provides comprehensive program management, program control, operations, analysis and administrative support for cyber security policy and information security initiatives.

The job functions are:

- Conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks and remedies
- Providing recommendations as an authoritative leader in the cyber security, networks, and networks operations arena
- Designing, architecting, and guiding the technical leadership and recommending solutions to the security problems in the existing systems and the systems under development
- Assisting with application of formal methodologies in security architecture, security system design and engineering to help with “security technology” integration and deployment
- Leading and participating in security tests, evaluations, and studies
| Experience                                                                 | This position requires 7+ years of experience in cyber security, cyber operations, information assurance, information security, technical analysis, or a combination thereof. The experience must include activities such as:  
  - Gathering, evaluating, and verifying vulnerability for information technology systems, networks, worldwide automated information systems  
  - Participating in the development or implementation of information security exercises  
  - Monitoring new and emerging information technologies, changes in professional and technical standards and advancements in technology for influence on information security practices  
  - Building and maintaining relationships and partnerships with the stakeholders to exchange security information and promote situational awareness  
  - Exceptional communication and writing skills, and the ability to draft technical documentations |
| Education                                                                 | This position requires a minimum of a baccalaureate degree in Computer Science or Information Systems from an accredited college or university or equivalent work experience. CISSP certification or equivalent is desired. |

### 7. Certification & Accreditation Specialist

| Responsibilities                                                                 | In this role, the candidate supports the creation, documentation and validation of information systems and the relevant security controls within. It identifies and documents the confidentiality, integrity and availability of all IT assets and data. The job functions are:  
  - Completing initial FIPS 199 Categorization for selected General Support System (GSS), Major or Minor Applications  
  - Completing initial Privacy Impact Assessment for selected General Support System (GSS), Major or Minor Applications  
  - Completing initial e-Authentication for selected General Support System (GSS), Major or Minor Applications  
  - Creating System Security Plan (SSP) for selected General Support System (GSS), Major or Minor Applications  
  - Submitting SSP to Capacity Planning (CP) Team for completion of Contingency Plan  
  - Assisting with Security Test and Evaluation (ST&E) planning and test execution  
  - Providing periodic internal Risk Assessment (RA) security reports to ISSO/DC2 Security Manager  
  - Documenting strategies and findings in the Security Assessment Report (SAR)  
  - Drafting Authorization to Operate (ATO) Letter for Information Systems Security Manager (ISSM)  
  - Drafting Plan of Action and Milestones (POA&M), SAR, and Vulnerability Scan reports  
  - Providing annual Self-Assessments reports to ISSM/ISSO and other management as needed |
## Experience
This position requires expert-level knowledge of:
- FIPS 199 Categorization
- FISMA Regulation
- NIST guidelines
- Privacy Impact Assessment
- e-Authentication
- System Security Plan (SSP)
- Security Test and Evaluation (ST&E) planning
- Risk Assessment (RA)
- Security Assessment Report (SAR)
- Authorization to Operate (ATO) Letter
- Plan of Action and Milestones (POA&M)
- Vulnerability Scan
- Self-Assessments reports

## Education
This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 5+ years of work experience. An active CISSP certification is preferred.

## 8. Software Developer

### Responsibilities
In this role, the candidate designs and develops software and web applications for medium to large organizations or government agencies, contributing to all aspects of the product development and release life-cycle. This position requires:
- Developing web applications for mission critical business functions
- Developing web applications based on principles and methodologies of SOA (Service Oriented Architectures)
- Expert-level familiarity with interoperable services
- Thorough understanding of data structures
- Expert-level familiarity with Microsoft-based frameworks and models for designing and developing web applications

### Experience
This position requires:
- Proven track record of successfully developing web applications using Microsoft technologies such as
  - ASP.NET, SharePoint, Dynamics, BizTalk etc.
- Developing solutions based on .NET platform using C# and VB.NET
- Thorough understanding of relational database design and optimization
- Demonstrating proficiency in all aspects of the software development process including requirements gathering, design, implementation, debugging, and testing
- Researching and resolving challenging and complex technical and analytical problems
- Proficiency using SOAP and other (3rd party) API interface methods
- Leading teams and multiple work-streams

### Education
This position requires a minimum of 5+ years of experience and a BS/BA in Computer Information Technology, Computer Science, Management Systems, Management or a related discipline.
### Responsibilities

The Senior Technical Lead and Project Manager acts as a strategic leader to his/her organization and senior management by providing creative and innovative technology solutions that will improve the overall representative and customer experience and lower the total cost of ownership. Team members work in a fast-paced environment delivering both tactical and strategic technology solutions. This position requires:

- Directing and guiding daily software development activities and acting as a hands-on delivery leader
- Developing project plans and scope including time estimates based on functional requirements; monitoring and supervising the assigned team of technical professionals
- Coordinating the evolution of technical designs and code components to support detailed specifications and functional/non-functional requirements
- Participating directly with various staff in the creation of end-to-end architecture, technical designs and code components for enterprise-level, scalable applications
- Ensuring development of reusable code design, leveraging application architecture/framework capabilities and functionalities
- Ensuring that coding standards are being followed and that regular code reviews are performed
- Ensuring test cases are being written and executed and drive testing automation for assigned areas
- Working with other teams to coordinate deliverables
- Identifying potential issues and risks to solve technical hurdles
- Formulating options to mitigate issues and risks
- Mentoring team members
- Supporting (individual) professional development plans
- Conducting performance evaluation and providing feedback to team members
- Preparing and providing verbal and written status reports as necessary required
- Performing other duties as necessary or as assigned

### Experience

This position requires:

- 7+ years of experience in developing commercial software solutions for large enterprise applications and with corresponding SDLC concepts
- 7+ years of experience leading developers in the development of software products
- 7+ years of experience in object-oriented design and programming, web-based business application design and development and with hands-on ASP.NET/SQL Server development experience
- In-depth technical design experience - recruiting, managing and evaluating software engineers

### Education

This position requires a minimum of a baccalaureate degree in Computer Science or Information Systems from an accredited college or university or equivalent work experience. An active MCPD, MCTS, MTA and/or PMI certification is desired.
## 10. Cyber Security Lead and Project Manager

### Responsibilities
- Responsible for knowing where a network’s possible vulnerabilities lie.
- Staying on top of the methods cyber criminals use to infiltrate information systems and they use their expertise and knowledge to avert these efforts.
- Protect organizations from losing data, such as customers’ credit card information and valuable trade secrets, as well as the time and money lost when information systems are brought to a halt.
- Planning and implementing security measures on all information systems and networks
- If intrusion takes place, it is the cybersecurity manager’s job to take care of it as quickly and effectively as possible.

### Experience
- 15 years of related experience in information security with comprehensive knowledge of security automation, such as SCAP protocols.
- Establishing network security policies and procedures, regulating access to information and training staff on proper use of information systems.
- Monitoring systems for security gaps, design effective solutions and provide reports to management and executive staff.
- Running risk assessments, testing data processing systems and designing firewalls
- Experience with a wide variety of network security systems and centralized logging systems
- Experience applying system configuration settings in support of IA compliance
- Understanding of Incident Analysis

### Education
- Master’s Degree: Mid- and upper-level cybersecurity Managers often hold advanced degrees, such as the Master of Science in Information Assurance & Cybersecurity. An advanced degree typically takes an additional one to two years beyond the bachelor’s level.

## 11. Help Desk Support Service Specialist II

### Responsibilities
- Responds to telephone calls, email and personnel requests for technical support.
- Documents, tracks, and monitors the problem to ensure a timely resolution
- Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem.
- Simulates or recreates user problems to resolve operating difficulties.

### Experience
- 5 years as a Help Desk Specialist or equivalent experience

### Education
- BA or BS degree
<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>Experience</th>
<th>Education</th>
</tr>
</thead>
</table>
| • Technical and operational responsibility for the hardware, software, and systems under the Systems Engineering Team.  
• Perform installation, configuration, operational support and maintenance of Microsoft server operating systems in the data centers.  
• Manage and maintain the incident management queues for the Team  
• Work problem tickets and issues to completion  
• Provide metrics for Server Systems (e.g. availability, backup, patching).  
• Adhere to compliance controls as assigned (e.g. Internal Security Audits).  
• Work with Managed Service Providers and provide oversight for Service Level Agreement adherence.  
• Maintain a highly available and scalable computing environment.  
• Assist with technical issues, project management, design, analysis and implementation of computing solutions as needed.  
• Develop and execute mitigation plans for technical issues.  
• Prepare periodic maintenance plans and comply with change management procedures.  
• Maintain detailed knowledge of company server and technology standards.  
• Participate in 24x7 on call rotation.  

| • 7 years of Windows Server, Active Directory, and Exchange Server Administration.  
• 7 years of Microsoft Server technical experience.  
• Extensive experience supporting a large Exchange environment.  
• Microsoft Windows 2003 / 2008 / 2012 experience (Active Directory, DNS, DHCP, Clustering, IIS, GPO’s, and Windows Scripting).  
• Operations management of a Windows server environment – Backup, virus protection and remote office architecture.  
• Working knowledge of Cisco IP networks.  
• Experience supporting 24x7 production environments.  
• Experience with Hardware and Software virtualization.  
• Excellent communication skills, both written and verbal.  
• Ability to produce and adhere to documentation – Visio, run books, RFP’s, Project Plans and Root Cause Analysis.  
• SAN knowledge and experience is a plus.  
• Perform server hardware setup and configuration.  
• Support of Automated Server Deployments.  
• Support of Antivirus and Backup/Restore solutions.  
• Communicates effectively with internal clients to identify needs and evaluate alternative business solutions and strategies.  
• Ability to quickly understand and learn to support multiple hardware and software systems.  
• Ability to adapt to a fast paced, growing environment.  

| This position requires a minimum of a baccalaureate degree or higher in systems engineering, computer science, management information systems, or related field preferred from an accredited college or university or equivalent work experience. |
### 13. Web and Intranet Applications Specialist II

**Responsibilities**
- Develops, implements, and maintains web-based application systems for an organization.
- Troubleshoots issues with existing or developed systems, and works with the appropriate resources to resolve them.
- Relies on experience and judgment to plan and accomplish goals. Performs a variety of complicated tasks.
- Works under general supervision; typically reports to a supervisor or manager.

**Experience**
- 4 years of experience in the field or in a related area.

**Education**
- This position requires a minimum of a baccalaureate degree or higher in systems engineering, computer science, management information systems, or related field preferred from an accredited college or university or equivalent work experience.

### 14. Senior Project Manager

**Responsibilities**
- Serves as the project manager for a large, complex task order (or a group of task orders).
- Assists the Program Manager in working with the Government Contracting Officer (CO), the contract-level Contracting Officer's Representative (COR), the task order-level COR(s), government management personnel and customer agency representatives.
- Under the guidance of the Program Manager, responsible for the overall management of the specific task order(s) and ensuring that the technical solutions and schedules in the task order are implemented in a timely manner.
- Works under general supervision; typically reports to a supervisor or manager.

**Experience**
- This position requires 12 years’ experience of which at least nine years must be specialized.
- Specialized experience includes: project development from inception to deployment, expertise in the management and control of resources, demonstrated capability in managing multi-task contracts and/or subcontracts of various types and complexity.
- General experience includes increasing responsibilities in information systems design and/or management.

**Education**
- A Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related discipline.
- With a Master's Degree, ten years of general experience of which at least seven years must be specialized.
- With a Ph.D., eight years of general experience of which at least six years must be specialized.
- With fifteen years general experience, of which at least twelve years specialized experience, a degree is not required.
<table>
<thead>
<tr>
<th><strong>15. Software Developer II</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>- Codes software applications to adhere to designs supporting internal business requirements or external customers.</td>
</tr>
<tr>
<td>- Document every aspect of the application or system as a reference for future maintenance and upgrades.</td>
</tr>
<tr>
<td>- Ensure that the software continues to function normally through software maintenance and testing.</td>
</tr>
<tr>
<td>- Standardizes the quality assurance procedure for software.</td>
</tr>
<tr>
<td>- Oversees testing and develops fixes.</td>
</tr>
<tr>
<td>- Performs a variety of tasks.</td>
</tr>
<tr>
<td>- Works under general supervision.</td>
</tr>
<tr>
<td>- A certain degree of creativity and latitude required.</td>
</tr>
<tr>
<td>- Typically reports to a project leader or manager.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>- Has knowledge of standard concepts, practices, and procedures within a particular field.</td>
</tr>
<tr>
<td>- Relies on experience and judgment to plan and accomplish goals.</td>
</tr>
<tr>
<td>- 3 years of experience in the field or in a related area.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>- Require a bachelor's degree in a related area.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>16. Web Application Developer II</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>In this role, the candidate designs and develops public-facing web applications for medium to large organizations or government agencies, contributing to all aspects of the product development and release life-cycle. This position requires:</td>
</tr>
<tr>
<td>- Developing web applications for mission critical business functions.</td>
</tr>
<tr>
<td>- Developing web applications based on principles and methodologies of SOA (Service Oriented Architectures).</td>
</tr>
<tr>
<td>- Expert-level familiarity with interoperable services.</td>
</tr>
<tr>
<td>- Thorough understanding of data structures.</td>
</tr>
<tr>
<td>- Expert-level familiarity with Microsoft-based frameworks and models for designing and developing web applications.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>This position requires:</td>
</tr>
<tr>
<td>- 4 years’ experience.</td>
</tr>
<tr>
<td>- Proven track record of successfully developing web applications using Microsoft technologies such as ASP.NET, SharePoint, Dynamics, BizTalk etc.</td>
</tr>
<tr>
<td>- Developing solutions based on .NET platform using C# and VB.NET.</td>
</tr>
<tr>
<td>- Thorough understanding of relational database design and optimization.</td>
</tr>
<tr>
<td>- Demonstrating proficiency in all aspects of the software development process including requirements gathering, design, implementation, debugging, and testing.</td>
</tr>
<tr>
<td>- Researching and resolving challenging and complex technical and analytical problems.</td>
</tr>
<tr>
<td>- Proficiency using SOAP and other (3rd party) API interface methods.</td>
</tr>
<tr>
<td>- Leading teams and multiple work-streams.</td>
</tr>
<tr>
<td>Education</td>
</tr>
<tr>
<td>-----------</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>17. Database Application Developer II</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Installation, configuration and upgrading of Oracle server software and related products</td>
</tr>
<tr>
<td></td>
<td>• Evaluate Oracle features and Oracle related products</td>
</tr>
<tr>
<td></td>
<td>• Establish and maintain sound backup and recovery policies and procedures</td>
</tr>
<tr>
<td></td>
<td>• Take care of the Database design and implementation</td>
</tr>
<tr>
<td></td>
<td>• Implement and maintain database security (create and maintain users and roles, assign privileges)</td>
</tr>
<tr>
<td></td>
<td>• Perform database tuning and performance monitoring</td>
</tr>
<tr>
<td></td>
<td>• Perform application tuning and performance monitoring</td>
</tr>
<tr>
<td></td>
<td>• Setup and maintain documentation and standards</td>
</tr>
<tr>
<td></td>
<td>• Plan growth and changes (capacity planning)</td>
</tr>
<tr>
<td></td>
<td>• Work as part of a team and provide 7x24 support when required</td>
</tr>
<tr>
<td></td>
<td>• Perform general technical trouble shooting and give consultation to development teams</td>
</tr>
<tr>
<td></td>
<td>• Interface with Oracle Corporation for technical support.</td>
</tr>
<tr>
<td></td>
<td>• Patch Management and Version Control</td>
</tr>
</tbody>
</table>

| Experience | May be certified as an Oracle DBA. See Oracle Certification Program. Must have 7 years’ |
| Education  | Preferably a BS in computer science or related engineering field |

<table>
<thead>
<tr>
<th>18. Software QA Analyst III</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Develops, publishes, and implements test plans.</td>
</tr>
<tr>
<td></td>
<td>• Writes and maintains test automation.</td>
</tr>
<tr>
<td></td>
<td>• Develops quality assurance standards.</td>
</tr>
<tr>
<td></td>
<td>• Defines and tracks quality assurance metrics such as defect densities and open defect counts.</td>
</tr>
<tr>
<td></td>
<td>• Performs a variety of tasks.</td>
</tr>
<tr>
<td></td>
<td>• May lead and direct the work of others.</td>
</tr>
<tr>
<td></td>
<td>• Works under general supervision; typically reports to a manager.</td>
</tr>
<tr>
<td></td>
<td>• A certain degree of creativity and latitude is required.</td>
</tr>
</tbody>
</table>

| Experience | At least 5 years of experience coding in C, C++, Java. |
|           | Must have a working knowledge of quality assurance methodologies. |
|           | Familiar with NT, UNIX and/or Solaris environments. |
|           | Relies on experience and judgment to plan and accomplish goals |

| Education  | Requires a bachelor's degree |
### 19. Database Administrator II

**Responsibilities**

- Provides technical expertise in the use of DBMS.
- Evaluates and recommends available DBMS products to support validated user requirements.
- Defines file organization, indexing methods, and security procedures for specific user applications.

**Experience**

- This position requires a minimum of six years’ experience, of which at least four years must be specialized.
- Specialized experience includes experience using current DBMS technologies, and application design utilizing various DBMS.
- General experience includes increasing responsibilities in DBMS systems analysis and programming.

**Education**

- A Bachelor's degree in Computer Science, Information Systems, Engineering, or other related discipline.
- With a Master's Degree, four years general experience of which at least three years must be specialized.
- With ten years of general experience of which at least eight years must be specialized experience, a degree is not required.

### 20. Cloud Computing Architect

**Responsibilities**

- Expert guidance to allow mid-size and enterprise companies to operate in the cloud more efficiently, decrease risk and increase profitability
- Designing solutions to help customers and partners solve technical problems
- Helping companies understand application architectures and integration approaches, and the consultative and leadership skills
- Should be familiar with security best practices for applications, servers, and networks
- Help shape and deliver on a broad use of utility computing web resources
- Owning the technical engagement and ultimate success around specific implementation projects
- Developing a deep expertise in the AWS technologies
- Being a subject matter expert on security as it relates to customer applications and services.

**Experience**

- Must have 12 years’ experience.
- Highly technical experience with large server and application deployments and virtualization
- Experience working within the software development or Internet industries is highly desired
- Working knowledge of software development practices and technologies highly desired.
- Experience designing solutions with technologies like: MSSQL, Windows Server 2003/2008/2012, IIS 7 & 8, Exchange, Active Directory, VMWare, Hyper-V, etc.
- Should have experience designing solutions with multiple distro’s (RHEL, CentOS, etc), Apache, MySQL, Tomcat, OpenVZ, VMware,ext.
- Working knowledge of AWS and/or Azure, or experience building High-Availability or High Traffic infrastructure would be preferred.
### Education
- Must have a bachelor's degree
- Industry certifications; ex: Microsoft Certified IT Professional
- Technical degree preferred; Computer Science or Math background highly desired.

### 21. Cyber Security Architect

#### Responsibilities
- Establish a unified approach and methodology for design, development, documentation, verification, training and stakeholder engagement for reference architectures for cyber security across the civilian federal government. Must have the capability to:
  - Develop a process to collect agency needs and best practices
  - Develop training and engagement plan for all reference architectures
  - Identify key areas of concern of the federal government's reference architecture structure
  - Identify gaps in core capabilities
  - Present findings and recommendations to multi-agency working groups
  - Develop future metrics
  - Supporting the Architecture Topology Alignment (ATA) strategic initiative, to provide executive departments and agencies with a robust service architecture to automate the identification of security risks and vulnerabilities across an enterprise topology.
  - Development, design and pilot testing

#### Experience
- 10 years of related experience in information security with comprehensive knowledge of security automation, such as SCAP protocols.
- Experience identifying and evaluating COTS products and toolsets that provide enterprise services in a complex IT environment
- Experience developing and refining technical processes and workflows to remove shortcomings and enhance customer efficiencies
- Experience with datacenter management, security and systems monitoring tools

#### Education
- MS in Engineering/Computer Science/Information Systems

### 22. Business Intelligence Analyst II

#### Responsibilities
- Collaborate to perform data and process analyses required
- Procure buy in from stakeholders
- Define requirements and provide simplified explanations
- Synthesize data and feedback from users, clients, and management
- Contribute to short and long-term goal setting
- Develop action plans and aide in accountability
- Collaborate regularly with various teams, including market analytics
- Develop and utilize dashboards effectively
- Develop, analyze, and modify processes, data structures, and models
- Interact with clients to evaluate products and performance
- Maintain objectivity at all times to ensure processes and products are relevant
### Experience
- Minimum of 3-5 years’ experience working in analytics or relevant field
- Solid computer skills, including Microsoft Office, databases, web-based applications
- Significant work experience with Agile sprints, SQL, and HTML
- Keen eye for details and aptitude for working with data
- Highly accurate and thorough in all tasks
- Exceptional organizational and presentation skills
- Highly organized and able to prioritize tasks
- Outstanding written, verbal, and interpersonal skills
- Strong problem-solving skills and an analytical mind
- Proven experience as a collaborative team player
- Able to thrive in a fast-paced, deadline-driven environment

### Education
Bachelor’s degree in a relevant field required, master’s degree preferred

### 23. Business Intelligence Analyst III

### Responsibilities
- Collaborate to perform data and process analyses required
- Procure buy in from stakeholders
- Define requirements and provide simplified explanations
- Synthesize data and feedback from users, clients, and management
- Contribute to short and long-term goal setting
- Develop action plans and aide in accountability
- Collaborate regularly with various teams, including market analytics
- Develop and utilize dashboards effectively
- Develop, analyze, and modify processes, data structures, and models
- Interact with clients to evaluate products and performance
- Maintain objectivity at all times to ensure processes and products are relevant
- Make data-driven decisions and recommendations
- Articulately and concisely explain the implications of complex data

### Experience
- Minimum of 5 years’ experience working in analytics or relevant field
- Solid computer skills, including Microsoft Office, databases, web-based applications
- Significant work experience with Agile sprints, SQL, and HTML
- Significant experience with Tableau,
- Keen eye for details and aptitude for working with data
- Highly accurate and thorough in all tasks
- Exceptional organizational and presentation skills
- Highly organized and able to prioritize tasks
- Outstanding written, verbal, and interpersonal skills
- Strong problem-solving skills and an analytical mind
- Proven experience as a collaborative team player
- Able to thrive in a fast-paced, deadline-driven environment

### Education
Bachelor’s degree in a relevant field required, master’s degree preferred
| Responsibilities | • Work on design, development, and implementation of data warehousing, reporting and analytics solutions  
• Deliver strategy for transitioning current solutions into well integrated SSAS cubes  
• Suggest new ideas for data visualization (SSRS/ Power BI)  
• Advanced relational data modeling and database design (SQL Server, MS Access)  
• Multidimensional modeling and experience building and fine tuning OLAP cubes (SSAS)  
• Data transformation and ETL (SSIS)  
• Hands on with Power BI Desktop and Power BI Cloud services.  
• Report development and troubleshooting experience Proficiency with the Microsoft Office Suite with a strong emphasis on Excel (Pivot tables, formulas and data extraction/manipulation)  
• Development with SSIS Experience including Microsoft SQL Server 2014 or newer, Analysis Services, Reporting Services, Integration Services, and Excel. |
| Experience | • Minimum 5 years of professional experience analyzing data Strong understanding of Power BI features and capabilities.  
• Added advantage who has knowledge other Microsoft technologies like SSRS, Azure. Microsoft Power BI (2+ years) Microsoft Power Query (2+ years) M query language (2+ years) Data Modeling / Relationship building (5+ years) Data transformations (measures, calculated columns, joins) (5+ years)  
• Expertise in creating dynamic reports and complex dashboards, ability to extract data from different data sources, analyze the reports for any data inconsistency and able to share data insights with IT and Business teams.  
• Experience creating dashboards and reports with Power BI Writing complex reports with ETL  
• Experience with the T-SQL scripting/programming language, including the ability to develop, test, tune, and debug ad-hoc queries, stored procedures and data migration script  
• Advanced experience with Microsoft Excel (Pivot, PowerPivot, VBA highly desired) |
<p>| Education | Bachelor’s degree in a relevant field required, master’s degree preferred |</p>
<table>
<thead>
<tr>
<th>Responsibilities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Designing, launching, and operating cloud services in one or more cloud services providers</td>
<td></td>
</tr>
<tr>
<td>• Designing and deploying applications using service-oriented architecture design patterns including enterprise service bus and related technologies</td>
<td></td>
</tr>
<tr>
<td>• Writing and implementing technical use cases</td>
<td></td>
</tr>
<tr>
<td>• Developing and leading software development efforts using agile software development techniques with a preference for Scrum</td>
<td></td>
</tr>
<tr>
<td>• Migrating applications from data centers to clouds</td>
<td></td>
</tr>
<tr>
<td>• Migrating applications from use of stand-alone servers to managed services</td>
<td></td>
</tr>
<tr>
<td>• Understanding of federal contracting rules to include Federal Acquisition Regulations including departmental supplements and additional guidance</td>
<td></td>
</tr>
<tr>
<td>• Familiarity with one of more software packages or service offerings used to dynamically launch and configure cloud service provider services</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Operating experience to include configuring and starting services in at least one cloud service provider, preferably Amazon Web Services (AWS) or Terremark</td>
<td></td>
</tr>
<tr>
<td>• Software engineering experience to include object-oriented design and development in at least one object-oriented language with Java Enterprise Edition and Ruby-on-Rails preferred</td>
<td></td>
</tr>
<tr>
<td>• Experience with designing and deploying distributed authentication mechanisms using Service Assertion Markup Language version 2.0</td>
<td></td>
</tr>
<tr>
<td>• Demonstrated development skills using scripting languages to include Linux shell scripting and other scripting languages including php and python</td>
<td></td>
</tr>
<tr>
<td>• Demonstrated skills in the use of AWS service configuration and choreography to include CloudFormation and DevOps</td>
<td></td>
</tr>
</tbody>
</table>

| Education                                                                 | This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 10 years' experience. |
### 26. Cloud Computing Lead & Project Manager

**Responsibilities**
- PCI familiarity
- Detailed knowledge of ISO 27001 Info Security standard
- Active Directory familiarity
- Translate requirements from user into detailed action plans
- Implement these detailed actions plans
- Provide period project status reports to stakeholders
- Proactively plan and keep projects on schedule
- Lead cross functional project teams
- Developing and maintaining operating level relationships with key executives at our suppliers for delivery of service
- Negotiating Master Services Agreements and Statements of Works with new approved suppliers
- Managing other supplier management personnel who support the other towers within Supplier Management (e.g. network, telecom, hardware/software category managers)

**Experience**
- Minimum 8 years of experience in negotiating agreements with infrastructure providers preferably in the Data Center, Hosting and Cloud Computing space.
- Minimum 8 years of experience in demonstrating ability to remove cost from IT 3rd party spends and operations with Fortune 1000 level companies.
- Minimum 5 years of experience with current and past vendor contracting and licensing models and experience with migrating from fixed fee to utility service models
- Minimum 5 years of financial experience in reconciling financial spends with contract management spend.
- Minimum 8 years of experience in the infrastructure services market, pricing, service levels, terms and conditions, benchmarking processes, data privacy, and provider market space.
- Minimum 5 years of client sales support experience in delivering the message of how savings will be delivered and achieved.
- Advanced experience managing complete cloud delivery projects

**Education**
- PMP highly desired
- BS/BA degree or equivalent work experience combined with a minimum of 15 years relevant industry experience in software, hardware (more server than storage) and/or consulting services sales.

### 27. Database Administrator I

**Responsibilities**
- Provides technical support in the use of DBMS products for user requirements.
- Defines file organization, indexing methods, and security procedures for specific user applications.

**Experience**
- This position requires a minimum of three years’ experience, of which at least two years must be specialized.
- Specialized experience includes experience using current DBMS technologies, and application design utilizing various DBMS.
- General experience includes responsibilities in DBMS systems analysis and programming.
| Education | • Bachelor's degree in Computer Science, Information Systems, Engineering, or other related discipline.  
• With six years of general experience of which at least four years must be specialized experience, a degree is not required. |
|---|---|
| **28. Help Desk Support Service Specialist III** | **Responsibilities** | • Provides second-tier support to end users for both PC, server, or mainframe applications and hardware.  
• Interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem.  
• Simulates or recreates user problems to resolve operating difficulties.  
• Recommends systems modifications to reduce user problems |
| Experience | 7+ years as a Help Desk Specialist or equivalent experience |
| Education | BA or BS degree |
| **29. Information Security SME** | **Responsibilities** | In this role, the candidate supports the development and implementation of IT Security controls that adhere to NIST guidelines. It supports the development and implementation policies and standards in regards to information systems and data within a datacenter. It ensures confidentiality, integrity and availability of all IT assets and data. This position requires:  
• Ensuring the implementation, integrity and monitoring of security controls in accordance with the SSP and NIST policies and procedures  
• Conducting and participating in annual security assessments  
• Conducting and participating in security audits  
• Providing security guidance to designated design and engineering personnel for service development  
• Completing security controls verification for General Support System (GSS), Major or Minor Applications  
• Completing security controls validation for General Support System (GSS), Major or Minor Applications  
• Implementing policies, procedures and process reviews for General Support System (GSS), Major or Minor Applications  
• Completing regular and periodic compliance/vulnerability scan assessments for General Support System (GSS), Major or Minor Applications |
<table>
<thead>
<tr>
<th>Experience</th>
<th>This position requires expert-level knowledge of:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• FIPS 199 Categorization</td>
</tr>
<tr>
<td></td>
<td>• FISMA Regulation</td>
</tr>
<tr>
<td></td>
<td>• NIST guidelines</td>
</tr>
<tr>
<td></td>
<td>• Privacy Impact Assessment</td>
</tr>
<tr>
<td></td>
<td>• e-Authentication</td>
</tr>
<tr>
<td></td>
<td>• System Security Plan (SSP)</td>
</tr>
<tr>
<td></td>
<td>• Security Test and Evaluation (ST&amp;E) planning</td>
</tr>
<tr>
<td></td>
<td>• Risk Assessment (RA)</td>
</tr>
<tr>
<td></td>
<td>• Security Assessment Report (SAR)</td>
</tr>
<tr>
<td></td>
<td>• Authorization to Operate (ATO) Letter</td>
</tr>
<tr>
<td></td>
<td>• Plan of Action and Milestones (POA&amp;M)</td>
</tr>
<tr>
<td></td>
<td>• Vulnerability Scan</td>
</tr>
<tr>
<td></td>
<td>• Self-Assessments reports</td>
</tr>
</tbody>
</table>

| Education | This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 4-5 years of work experience. An active CISSP certification is preferred. |

<table>
<thead>
<tr>
<th>30. Information Systems Security Officer (ISSO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibilities</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience</th>
<th>Must have at least 5 years’ experience serving as an ISSO for a major system</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Intimately familiar with NIST SP800-53 and FISMA requirements</td>
</tr>
<tr>
<td></td>
<td>Experience developing, tracking and managing POA&amp;Ms</td>
</tr>
<tr>
<td></td>
<td>Experience developing system/application C&amp;A documentation (SSP, CP, CMP, SCA reports, etc.)</td>
</tr>
<tr>
<td></td>
<td>Experience interpreting IT vulnerability scanning results</td>
</tr>
<tr>
<td></td>
<td>Risk assessment experience, especially with NIST 800-30 threat identification, system security categorization, gap analysis, compliance reporting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Education</th>
<th>Must have a Bachelor's Degree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Certifications: CISSP and CAP</td>
</tr>
</tbody>
</table>
### 31. Project Manager I

**Responsibilities**
- Serves as the project manager for a medium size task or contract.
- Assists in working with the contract-level Contracting Officer's Representative (COR), and government management personnel and customer agency representatives.
- Under the guidance of the Program Manager, responsible for ensuring that specific tasks and schedules are implemented in a timely manner.

**Experience**
- This position requires a minimum of five years’ experience of which at least three years must be specialized.
- Specialized experience includes project deployment, management of resources, and managing contracts and/or subcontracts.
- General experience includes increasing responsibilities in information systems design and/or management.

**Education**
No Degree is required

### 32. Project Manager II

**Responsibilities**
- Serves as the project manager for a large task order or contract.
- Assists in working with the Government Contracting Officer (CO), the contract-level Contracting Officer's Representative (COR), and government management personnel and customer agency representatives.
- Under the guidance of the Program Manager, responsible for management of the specific

**Experience**
- This position requires a minimum of seven years’ experience of which at least five years must be specialized.
- Specialized experience includes project development from inception to deployment, expertise in the management of resources, managing contracts and/or subcontracts of various types and complexity.

**Education**
- A Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related discipline.
- Ten years general experience of which at least eight years specialized experience, a degree is not required.
### 33. Software Engineer II

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Determines operational feasibility by evaluating analysis, problem definition, requirements, solution development, and proposed solutions.</td>
</tr>
<tr>
<td></td>
<td>Documents and demonstrates solutions by developing documentation, flowcharts, layouts, diagrams, charts, code comments and clear code.</td>
</tr>
<tr>
<td></td>
<td>Prepares and installs solutions by determining and designing system specifications, standards, and programming.</td>
</tr>
<tr>
<td></td>
<td>Improves operations by conducting systems analysis; recommending changes in policies and procedures.</td>
</tr>
<tr>
<td></td>
<td>Obtains and licenses software by obtaining required information from vendors; recommending purchases; testing and approving products.</td>
</tr>
<tr>
<td></td>
<td>Updates job knowledge by studying state-of-the-art development tools, programming techniques, and computing equipment; participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.</td>
</tr>
<tr>
<td></td>
<td>Protects operations by keeping information confidential.</td>
</tr>
<tr>
<td></td>
<td>Provides information by collecting, analyzing, and summarizing development and service issues.</td>
</tr>
<tr>
<td></td>
<td>Accomplishes engineering and organization mission by completing related results as needed.</td>
</tr>
<tr>
<td></td>
<td>Develops software solutions by studying information needs; conferring with users; studying systems flow, data usage, and work processes; investigating problem areas; following the software development lifecycle.</td>
</tr>
</tbody>
</table>

| Experience | Develops information systems by designing, developing, and installing software solutions. Software engineers are responsible for the complete life cycle of a new/modified software product, from research and design to implementation, training and support. |

| Education | Bachelor of Science Degree in Computer Science, Electrical Engineering, Computer Engineering, Aerospace Engineering, Math or Physics or a technical field (such as CIS or IT) AND a minimum of one year relevant experience OR an equivalent combination of education and relevant experience. |
|           | Demonstrates proficient knowledge and utilization of engineering tools necessary for successful performance of the essential functions of this job description. |
|           | Must demonstrate proficiency and possess experience necessary to develop moderately complex software in C, C++, C#, Java, assembly language, or other selected languages. |
|           | Demonstrates mastery of relevant software engineering tools (configuration management systems, build processes, debuggers, emulators, simulators and logic analyzers). |
|           | Must demonstrate proficient ability to capture and document software requirements. |
### Responsibilities
- Determines operational feasibility by evaluating analysis, problem definition, requirements, solution development, and proposed solutions.
- Documents and demonstrates solutions by developing documentation, flowcharts, layouts, diagrams, charts, code comments and clear code.
- Prepares and installs solutions by determining and designing system specifications, standards, and programming.
- Improves operations by conducting systems analysis; recommending changes in policies and procedures.
- Obtains and licenses software by obtaining required information from vendors; recommending purchases; testing and approving products.
- Updates job knowledge by studying state-of-the-art development tools, programming techniques, and computing equipment; participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations.
- Protects operations by keeping information confidential.
- Provides information by collecting, analyzing, and summarizing development and service issues.
- Accomplishes engineering and organization mission by completing related results as needed.
- Develops software solutions by studying information needs; conferring with users; studying systems flow, data usage, and work processes; investigating problem areas; following the software development lifecycle.

### Experience
Develops information systems by designing, developing, and installing software solutions. Software engineers are responsible for the complete life cycle of a new/modified software product, from research and design to implementation, training and support.

### Education
Bachelor of Science Degree in Computer Science, Electrical Engineering, Computer Engineering, Aerospace Engineering, Math or Physics or a technical field (such as CIS or IT) AND a minimum of one-year relevant experience OR an equivalent combination of education and relevant experience.
- Demonstrates proficient knowledge and utilization of engineering tools necessary for successful performance of the essential functions of this job description.
- Must demonstrate proficiency and possess experience necessary to develop moderately complex software in C, C++, C#, Java, assembly language, or other selected languages.
- Demonstrates mastery of relevant software engineering tools (configuration management systems, build processes, debuggers, emulators, simulators and logic analyzers).
- Must demonstrate proficient ability to capture and document software requirements.
<table>
<thead>
<tr>
<th>35. Software QA Analyst I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>- Develops, publishes, and implements test plans.</td>
</tr>
<tr>
<td>- Writes and maintains test automation.</td>
</tr>
<tr>
<td>- Develops quality assurance standards.</td>
</tr>
<tr>
<td>- Defines and tracks quality assurance metrics such as defect densities and open defect counts.</td>
</tr>
<tr>
<td>- Performs a variety of tasks.</td>
</tr>
<tr>
<td>- Works under general supervision; typically reports to a manager.</td>
</tr>
<tr>
<td>- A certain degree of creativity and latitude is required.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>- 0-2 years of experience coding in C, C++, Java.</td>
</tr>
<tr>
<td>- Must have a working knowledge of quality assurance methodologies.</td>
</tr>
<tr>
<td>- Relies on experience and judgment to plan and accomplish goals.</td>
</tr>
<tr>
<td>- Familiar with NT, UNIX and/or Solaris environments.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Requires a bachelor's degree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>36. Software QA Analyst II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>- Develops, publishes, and implements test plans.</td>
</tr>
<tr>
<td>- Writes and maintains test automation.</td>
</tr>
<tr>
<td>- Develops quality assurance standards.</td>
</tr>
<tr>
<td>- Defines and tracks quality assurance metrics such as defect densities and open defect counts.</td>
</tr>
<tr>
<td>- Performs a variety of tasks.</td>
</tr>
<tr>
<td>- Works under general supervision; typically reports to a manager.</td>
</tr>
<tr>
<td>- A certain degree of creativity and latitude is required.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>- 2-4 years of experience coding in C, C++, Java.</td>
</tr>
<tr>
<td>- Must have a working knowledge of quality assurance methodologies.</td>
</tr>
<tr>
<td>- Familiar with NT, UNIX and/or Solaris environments.</td>
</tr>
<tr>
<td>- Relies on experience and judgment to plan and accomplish goals.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Requires a bachelor's degree</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>37. Systems Engineer I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>- Responsible for the planning and engineering of an organization's systems infrastructure.</td>
</tr>
<tr>
<td>- Includes the implementation and design of hardware and software. Monitors the performance of systems.</td>
</tr>
<tr>
<td>- Works under general supervision. A certain degree of creativity and latitude is required.</td>
</tr>
<tr>
<td>- Typically reports to a supervisor or manager.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td>- 0-2 years of experience in the field or in a related area.</td>
</tr>
<tr>
<td>- Familiar with standard concepts, practices, and procedures within a particular field.</td>
</tr>
<tr>
<td>- Relies on limited experience and judgment to plan and accomplish goals.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
<tr>
<td>Typically requires a bachelor's degree in area of specialty</td>
</tr>
</tbody>
</table>
### 38. Systems Engineer II

**Responsibilities**
- Responsible for the planning and engineering of an organization's systems infrastructure.
- Includes the implementation and design of hardware and software.
- Monitors the performance of systems.
- Works under general supervision.
- A certain degree of creativity and latitude is required.
- Typically reports to a supervisor or manager.

**Experience**
- 2-4 years of experience in the field or in a related area
- Relies on limited experience and judgment to plan and accomplish goals.
- Familiar with standard concepts, practices, and procedures within a particular field.

**Education**
- Typically requires a bachelor's degree in area of specialty

### 39. Technical Writer I

**Responsibilities**
- Design, create, and maintain technical documentation. This documentation includes online help, user guides, Instructions for user manuals, white papers, design specifications, system manuals etc.
- Write, publish and maintain high-quality documentation and online content, and ensure material is accessible to customers
- Participate in various aspects of the documentation development cycle.
- Edit, standardize, or make changes to material prepared by other writers or establishment personnel.
- Confer with customer representatives, vendors, plant executives, or publisher to establish technical specifications and to determine subject material to be developed for publication.
- Analyze developments in specific field to determine need for revisions in previously published materials and development of new material.
- Review published materials and recommend revisions or changes in scope, format, content, and methods of reproduction and binding.

**Experience**
- Motivated to work independently and as part of a collaborative cross-functional team
- Comfortable using authoring tools, such as Adobe FrameMaker, Robohelp, AuthorIT, Flare, Adobe Acrobat, CS5, and MS Office
- Passion for learning and technology
- Experience in new media for information delivery (mobile formats, wikis, knowledge bases, web-delivered online-help)
- Ability to communicate complex concepts both visually and in words
- Ability to work on multiple projects at the same time.
- Ability to adjust quickly and smoothly to shifting customer needs and company priorities.
- Ability to interact positively and effectively with others including the ability to work well in a team environment

**Education**
- BA or BS degree
### Technical Writer II

<table>
<thead>
<tr>
<th><strong>Responsibilities</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Design, create, and maintain technical documentation. This documentation includes online help, user guides, Instructions for user manuals, white papers, design specifications, system manuals etc.</td>
<td></td>
</tr>
<tr>
<td>• Write, publish and maintain high-quality documentation and online content, and ensure material is accessible to customers</td>
<td></td>
</tr>
<tr>
<td>• Manage the production, publishing, and localization hand-off of your documentation</td>
<td></td>
</tr>
<tr>
<td>• Participate in various aspects of the documentation development cycle.</td>
<td></td>
</tr>
<tr>
<td>• Edit, standardize, or make changes to material prepared by other writers or establishment personnel.</td>
<td></td>
</tr>
<tr>
<td>• Confer with customer representatives, vendors, plant executives, or publisher to establish technical specifications and to determine subject material to be developed for publication.</td>
<td></td>
</tr>
<tr>
<td>• Analyze developments in specific field to determine need for revisions in previously published materials and development of new material.</td>
<td></td>
</tr>
<tr>
<td>• Review published materials and recommend revisions or changes in scope, format, content, and methods of reproduction and binding.</td>
<td></td>
</tr>
<tr>
<td>• Observe production, developmental, and experimental activities to determine operating procedure and detail.</td>
<td></td>
</tr>
<tr>
<td>• Meet with customer representatives, vendors, plant executives, or publishers to establish technical specifications.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Experience</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Excellent writing skills</td>
<td></td>
</tr>
<tr>
<td>• Proven teamwork and interpersonal skills</td>
<td></td>
</tr>
<tr>
<td>• Motivated to work independently and as part of a collaborative cross-functional team</td>
<td></td>
</tr>
<tr>
<td>• Comfortable using authoring tools, such as Adobe FrameMaker, Robohelp, AuthorIT, Flare, Adobe Acrobat, CS5, and MS Office</td>
<td></td>
</tr>
<tr>
<td>• Passion for learning and technology</td>
<td></td>
</tr>
<tr>
<td>• Experience in new media for information delivery (mobile formats, wikis, knowledge bases, web-delivered online-help)</td>
<td></td>
</tr>
<tr>
<td>• Ability to communicate complex concepts both visually and in words</td>
<td></td>
</tr>
<tr>
<td>• Ability to work on multiple projects at the same time.</td>
<td></td>
</tr>
<tr>
<td>• Ability to adjust quickly and smoothly to shifting customer needs and company priorities.</td>
<td></td>
</tr>
<tr>
<td>• Ability to interact positively and effectively with others including the ability to work well in a team environment</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Education</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• BA or BS degree</td>
<td></td>
</tr>
<tr>
<td>• 3+ years as a Technical Writer or equivalent experience</td>
<td></td>
</tr>
</tbody>
</table>
### 41. Technical Writer III

**Responsibilities**

- Design, create, and maintain technical documentation. This documentation includes online help, user guides, Instructions for user manuals, white papers, design specifications, system manuals etc.
- Gather resource material including specifications, schematics, technical presentations, original models, drawings, photography, first-hand observation, and the information and transform it into effective, usable product documentation.
- Write, publish and maintain high-quality documentation and online content, and ensure material is accessible to customers
- Manage the production, publishing, and localization hand-off of your documentation
- Participate in all aspects of documentation development, from product planning through product release
- Represent Technical Publications’ interests to internal customers
- Edit, standardize, or make changes to material prepared by other writers or establishment personnel.
- Confer with customer representatives, vendors, plant executives, or publisher to establish technical specifications and to determine subject material to be developed for publication.
- Analyze developments in specific field to determine need for revisions in previously published materials and development of new material.
- Review published materials and recommend revisions or changes in scope, format, content, and methods of reproduction and binding.
- Observe production, developmental, and experimental activities to determine operating procedure and detail.
- Study drawings, specifications, mockups, and product samples.
- Meet with customer representatives, vendors, plant executives, or publishers to establish technical specifications.

**Experience**

- Excellent writing skills
- Effective project management skills including planning and estimating project completion
- Proven teamwork and interpersonal skills
- Motivated to work independently and as part of a collaborative cross-functional team
- Comfortable using authoring tools, such as Adobe FrameMaker, Robohelp, AuthorIT, Flare, Adobe Acrobat, CS5, and MS Office
- Strong project management skills including planning and estimating project completion
- Ability to read wiring diagrams
- Passion for learning and technology
- Experience in new media for information delivery (mobile formats, wikis, knowledge bases, web-delivered online-help)
- Proficient skills in the authoring platforms mentioned above
- Ability to communicate complex concepts both visually and in words
- Ability to work on multiple projects at the same time.
- Ability to work with minimal direction and good communication skills are a must.
- Ability to adjust quickly and smoothly to shifting customer needs and company priorities.
- Ability to interact positively and effectively with others including the ability to work well in a team environment
### Education
- BA or BS degree
- 5+ years as a Technical Writer or equivalent experience

### 42. Web Application Developer I

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>In this role, the candidate designs and develops public-facing web applications for medium to large organizations or government agencies, contributing to all aspects of the product development and release life-cycle. This position requires:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Developing web applications for mission critical business functions</td>
</tr>
<tr>
<td></td>
<td>• Developing web applications based on principles and methodologies of SOA (Service Oriented Architectures)</td>
</tr>
<tr>
<td></td>
<td>• Expert-level familiarity with interoperable services</td>
</tr>
<tr>
<td></td>
<td>• Thorough understanding of data structures</td>
</tr>
<tr>
<td></td>
<td>• Expert-level familiarity with Microsoft-based frameworks and models for designing and developing web applications</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Experience</th>
<th>This position requires:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Proven track record of successfully developing web applications using Microsoft technologies such as ASP.NET, SharePoint, Dynamics, BizTalk etc.</td>
</tr>
<tr>
<td></td>
<td>• Developing solutions based on .NET platform using C# and VB.NET</td>
</tr>
<tr>
<td></td>
<td>• Thorough understanding of relational database design and optimization</td>
</tr>
<tr>
<td></td>
<td>• Demonstrating proficiency in all aspects of the software development process including requirements gathering, design, implementation, debugging, and testing</td>
</tr>
<tr>
<td></td>
<td>• Researching and resolving challenging and complex technical and analytical problems</td>
</tr>
<tr>
<td></td>
<td>• Proficiency using SOAP and other (3rd party) API interface methods</td>
</tr>
<tr>
<td></td>
<td>• Leading teams and multiple work-streams</td>
</tr>
</tbody>
</table>

| Education | This position requires a minimum of a baccalaureate degree in Computer Science or Information Systems from an accredited college or university or equivalent work experience. An active MCPD, MCTS or MTA certification is desired. |
# 43. Web Designer I

| Responsibilities | In this role, the candidate designs and develops web sites and web site components. The web designer designs, develops, tests and delivers web sites and web site components (e.g. graphics, logo, interactive forms etc.). Problem resolution and enhancements are part of the overall responsibilities. Using best practices and design methods, the web developer ensures the success of the final product. He/she builds the web site and components from the requirements stage, through design, testing and deployment to production. The designer is also responsible for creating graphics, logos, layout, scripting, programming, as well as development involving browser compatibility and seamless integration with various technologies ASP.NET, Java, J2EE, ColdFusion etc.
| |
| This position requires: |
| • Delivering exceptional web site design that substantiate preeminent usability and great look and feel |
| • Applying search engine optimization |
| • Designing web pages, graphics, multimedia and GUIs |
| • Developing in a clean, well-structured and easily maintainable navigation formats |
| • Storyboarding and scoping graphics pre-design where appropriate |
| • Demonstrating creative, technical and analytical skills |

| Experience | This position requires 5+ years of work experience in: |
| | • Developing websites and/or web applications |
| | • Understanding of navigation and GUI for maximizing usability |
| | • Front-end and some back-end development |
| | • Developing HTML, JavaScript, CSS, SQL, Perl, graphics creation with Photoshop, Illustrator, (Adobe Creative Suite), multimedia creation with Flash, ActionScript, (Macromedia Studio) |
| | • Using Active Server Pages, Java Server Pages and Java, XML, PHP, Oracle, MS SQL Server, ColdFusion Server, CFML, CFScript, IIS, Windows Server environments |

| Education | This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 5 years of work experience. |
### 44. Web Designer II

| Responsibilities | In this role, the candidate designs and develops web sites and web site components. The web designer designs, develops, tests and delivers web sites and web site components (e.g. graphics, logo, interactive forms etc.). Problem resolution and enhancements are part of the overall responsibilities. Using best practices and design methods, the web developer ensures the success of the final product. He/she builds the web site and components from the requirements stage, through design, testing and deployment to production. The designer is also responsible for creating graphics, logos, layout, scripting, programming, as well as development involving browser compatibility and seamless integration with various technologies ASP.NET, Java, J2EE, ColdFusion etc. This position requires:  
- Delivering exceptional web site design that substantiate preeminent usability and great look and feel  
- Applying search engine optimization  
- Designing web pages, graphics, multimedia and GUIs  
- Developing in a clean, well-structured and easily maintainable navigation formats  
- Storyboarding and scoping graphics pre-design where appropriate  
- Demonstrating creative, technical and analytical skills |
| Experience | This position requires 5+ years of work experience in:  
- Developing websites and/or web applications  
- Understanding of navigation and GUI for maximizing usability  
- Front-end and some back-end development  
- Developing HTML, JavaScript, CSS, SQL, Perl, graphics creation with Photoshop, Illustrator, (Adobe Creative Suite), multimedia creation with Flash, ActionScript, (Macromedia Studio)  
- Using Active Server Pages, Java Server Pages and Java, XML, PHP, Oracle, MS SQL Server, ColdFusion Server, CFML, CFScript, IIS, Windows Server environments |
| Education | This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 5 years of work experience. |
## 45. Oracle Application Developer (Technical) II

### Responsibilities
- Creates and maintains all databases required for development, testing, education and production usage.
- Performs the capacity planning required to create and maintain the databases. The DBA works closely with system administration staff because computers often have applications or tools on them in addition to the Oracle Databases.
- Performs ongoing tuning of the database instances.
- Install new versions of the Oracle RDBMS and its tools and any other tools that access the Oracle database.
- Plans and implements backup and recovery of the Oracle database.
- Controls migrations of programs, database changes, reference data changes and menu changes through the development life cycle.
- Implements and enforces security for all of the Oracle Databases.
- Performs database re-organizations as required to assist performance and ensure maximum uptime of the database.
- Puts standards in place to ensure that all application design and code is produced with proper integrity, security and performance. The DBA will perform reviews on the design and code frequently to ensure the site standards are being adhered to.
- Evaluates releases of Oracle and its tools, and third party products to ensure that the site is running the products that are most appropriate.

Planning is also performed by the DBA, along with the application developers and System administrators, to ensure that any new product usage or release upgrade takes place with minimal impact.

### Experience
- At least 4 years’ experience with business requirements gathering/analysis
- At least 3 years’ experience in systems design and development
- At least 3 years of cross-cultural experience preferred
- Experience with Oracle R12E-Business Suite modules such as GL, AP, AR, PO and FA preferred
- Experience of Oracle Development tools including:
  1. Oracle JDeveloper
  2. Oracle 10g Forms customization
  3. Oracle Workflow.
  4. Oracle 10g Reports.

### Education
- This opportunity requires either a Bachelor's degree in Computer Science, Information Systems, Computer Engineering or equivalent experience in the related field.
- Oracle certifications
### Responsibilities

Responsible for Oracle Development in an Oracle Applications environment in terms of design and development of Oracle based custom applications, interfaces, reports, and data conversions.

Experience with 10g Developer Suite for Forms and Reports, Oracle Application Framework (OAF), JDeveloper, Custom.pll and Forms Personalization, PL/SQL packages/procedures based programming for custom applications, data conversions, and interface development around Oracle EBS modules such as GL, AP, AR, PO and FA. Also desired is experience with Oracle Workflow Builder and developing new workflow and/or modifying existing workflows in either an Oracle Application or pure Oracle Technology environment. Must be knowledgeable in underlying Oracle Technology Stack and Oracle Applications database architecture with regard to E-Business Suite module schemas/products, standard (API's) application program interfaces, data elements, tables, and views as basis for troubleshooting, data conversion, interfaces, reporting and development.

- Participate in the development and maintenance of customizations of the Oracle Applications (Forms, Reports, PL/SQL, Discoverer queries) and deploying in Oracle environment.
- Participate in the development and maintenance of interfaces to and from the Oracle E-Business Applications.
- Deploying concurrent processes and custom development in Oracle Applications eBusiness Suite with use of System Administration and Application Developer module.
- Develop functional and technical design and documentation of Oracle Applications dependent data conversions, interfaces, custom reporting, and custom applications.

### Experience

- At least 5 years’ experience with business requirements gathering/analysis
- At least 4 years’ experience in systems design and development
- At least 4 years of cross-cultural experience preferred
- Experience with Oracle R12E-Business Suite modules such as GL, AP, AR, PO and FA preferred
- Experience of Oracle Development tools including:
  1. Oracle JDeveloper
  2. Oracle 10g Forms customization
  3. Oracle Workflow.
  4. Oracle 10g Reports.
  5. XML or BI Publisher.
  7. Noetix Views experience is a plus but not required
- Strong analytical and problem-solving skills.
- Oracle Technical Knowledge and Skills
- Prior experienced working on both Oracle Applications implementation.
- Advanced knowledge and understanding of information processing principles and practices
- Basic knowledge in core enterprise infrastructure
- Basic technical knowledge of network, PC, and platform operating systems with emphasis on A
### Education
- This opportunity requires either a Bachelor's degree in Computer Science, Information Systems, Computer Engineering or equivalent experience in the related field.
- Oracle certifications

### 47. Network Security Engineer I

| Responsibilities | • Perform all necessary functions associated with the implementation and integration of the customer’s technology environment.  
• Implement tactical plans to meet the Companies and Customer timelines and insure minimal disruption to the Customer environment.  
• Provide accurate, clear, concise documentation and assistance to others within the department when required. Assistance with development of documentation for standards requirements within the department.  
• Implement and maintains existing secure architectures for routing, switching, firewall, IDS/IPS, VPN, routing, and switching.  
• Assists in in-depth security related troubleshooting.  
• Assist with documentation and reporting for compliance efforts (PCI/ISO). |

| Experience | • Experience with Cisco VPN software and hardware configurations (2 to 3 years)  
• Familiar with Cisco Pix/ASA firewall configurations (2 to 3 years)  
• Experience with Sourcefire IDS/IPS (2 to 3 years)  
• Experience with Security best practices for routers/switches (2 to 3 years)  
• Minimum of 3-4 years of routing switching and security infrastructure. (2- to 3 years) |

| Education | • Bachelor’s Degree in a technological field and 1 years relevant experience. Bachelor’s Degree can be replaced by relevant experience on a year for year basis  
• CISSP certification or equivalent is desired |

### 48. Network Security Engineer II

| Responsibilities | • Provides recommendations (written reports when appropriate) in his/her area of authority and expertise  
• Performs technical design for network changes to existing or new hardware and software systems required to provide new functionality or enhance current performance and transition these changes to the operational environment  
• Mitigates the adverse impacts of service effecting issues on the business caused by network full or partial outages in the infrastructure and initiates actions to prevent recurrence of such issues  
• Proactively recommends and performs performance optimization activities to maximize efficiency and effectiveness of network resources  
• Performs risk management on a continual basis to ensure the identification and elimination of risks that can affect system availability, performance and reliability  
• Continually monitors the security of the network and ensures best practices have been implemented to thwart vulnerabilities of network attacks  
• Provides recommendations for new technology initiatives, standards and changes to the network or operating environment  
• Other duties as assigned |

| Experience | • Bachelor’s Degree in a technological field and 1 years relevant experience. Bachelor’s Degree can be replaced by relevant experience on a year for year basis  
• CISSP certification or equivalent is desired |
Experience

- Experience in enterprise network base lining, network capacity planning, security and network design and redesign
- 5+ years of experience supporting Cisco network equipment
- Monitoring/Remote Support: Experience in remote monitoring of system performance and remote client support
- Experience with routing and switching from both a Cisco and Brocade perspective
- Experience with Cisco or Avaya VOIP solutions
- Experience with monitoring solutions such as SolarWinds
- Working experience with Disaster Recovery planning, implementation and testing

Education

- Bachelor’s Degree in a technological field and 2 years relevant experience. Bachelor’s Degree can be replaced by relevant experience on a year for year basis
- CISSP certification or equivalent is desired

49. Network Security Engineer III

Responsibilities
In this role, the candidate architects and designs solutions for the network and network-related components as well as provides secure solutions for the datacenter operation. The job functions are:
- interfacing with customers to understand their Security requirements
- assisting in designing security solutions for customers
- developing firewall rule change requests
- creating firewall scripts
- verifying proper configuration and operation of firewalls
- verify proper configuration and operation of security agents
- troubleshooting network connectivity issues
- assisting with firewall capacity management
- providing second tier technical support for firewalls and security tools for the Security Operations Center (SOC)
- evaluating and making recommendations for security products to enhance security posture of the datacenter
- evaluating and making recommendations for datacenter change requests to ensure they comply with security standards

Experience
This position requires 7+ years of knowledge of:
- popular networking components like CISCO Firewall, Firewall Services Module (FWSM), ASA 5580 Series Appliances etc.
- VLAN/Trunking Protocol
- CISCO Catalyst 6509 Series Switches, Symantec Security Endpoint Security (SEC) and Critical System Protection (CSP)
- designing and deploying systems like typical 3-tier architecture web front-end, application back-end and databases etc.
- expert-level understanding of 7-layers of OSI model
- expert-level understanding of TCP/IP ports and protocols
- VMWare and VSphere
### Education
This position requires a minimum of a baccalaureate degree in Computer Science or Information Systems from an accredited college or university or equivalent work experience. CISSP certification or equivalent is desired.

### 50. Network Engineer II

#### Responsibilities
In this role, the candidate installs new computer hardware and systems software for networks and is responsible for overall administration and management of the network infrastructure. The job functions are:
- Installing, configuring and maintaining network services and devices
- Supporting administration of servers and server clusters
- Managing all system back-ups and restoring protocols
- Planning and supporting network and computing infrastructures
- Troubleshooting analysis of servers, workstations and associated components
- Documenting network problems and resolution for future reference
- Monitoring system performance and conducting performance tuning
- Setting up user accounts, permissions and passwords
- Managing user accounts, permissions, email, anti-virus, anti-spam etc.
- Monitoring network usage
- Overseeing software and network security

#### Experience
This position requires 5+ years of:
- Thorough knowledge of networking essentials
- Experience with Windows, CISCO’s family of networking devices, UNIX, Linux, Novell
- Hands-on experience with networking devices such as Switches, Routers, Hubs, Servers, Cables, Racks, Firewalls, LAN, WAN, TCP/IP, DNS, UDP, Latency, VoIP, QoS, OSPF, BGP, MPLS
- Advanced knowledge of 7-layers of OSI model
- Advanced knowledge of TCP/IP protocol suite

#### Education
This position requires a minimum of a baccalaureate degree or higher in Computer Science or Information System from an accredited college or university or equivalent work experience. One or more of MCSE, CCNA, CCNP, CCIE and CNE certification(s) is preferred.
### 51. Network Engineer III

#### Responsibilities

In this role, the candidate installs new computer hardware and systems software for networks and is responsible for overall administration and management of the network infrastructure. The job functions are:

- Installing, configuring and maintaining network services and devices
- Supporting administration of servers and server clusters
- Managing all system back-ups and restoring protocols
- Planning and supporting network and computing infrastructures
- Troubleshooting analysis of servers, workstations and associated components
- Documenting network problems and resolution for future reference
- Monitoring system performance and conducting performance tuning
- Setting up user accounts, permissions and passwords
- Managing user accounts, permissions, email, anti-virus, anti-spam etc.
- Monitoring network usage
- Overseeing software and network security

#### Experience

This position requires 5+ years of:

- Thorough knowledge of networking essentials
- Experience with Windows, CISCO’s family of networking devices, UNIX, Linux, Novell
- Hands-on experience with networking devices such as Switches, Routers, Hubs, Servers, Cables, Racks, Firewalls, LAN, WAN, TCP/IP, DNS, UDP, Latency, VoIP, QoS, EIGRP, BGP, OSPF, NHRP, ATM, PPP, MPLS
- Advanced knowledge of 7-layers of OSI model
- Advanced knowledge of TCP/IP protocol suite

#### Education

This position requires a minimum of a baccalaureate degree or higher in Computer Science or Information System from an accredited college or university or equivalent work experience. One or more of MCSE, CCNA, CCNP, CCIE and CNE certification(s) is preferred.

### 52. Oracle DBA I

#### Responsibilities

Responsible for oversight of multiple stand-alone Oracle database environments. The candidate must have excellent problem management, performance tuning experience and in-depth understanding of Oracle 10g, 11g concepts and best-practice administration standards. The candidate should have project upgrade and transition experience and be able to effectively communicate complex technical topics in summary form to various levels of management and client. The candidate will also participate in critical technical troubleshooting efforts and provide strategic technical advisement as warranted.

- Incident Management including root cause analysis and resolution of high impact/high visibility issues
- Design and execution on significant customer projects
- Participate in internal process and automation improvement opportunities
### Experience
- 3+ years of Oracle Database administration experience
- Thorough knowledge of the Oracle RDBMS, architecture, and technology stack
- Experience in sizing and architecting large scale environments including RAC based and ASM architecture
- Experience in installation, configuration and support; upgrade of Oracle to latest version
- Experience using Administration, Diagnostic and Tuning capabilities of OEM
- Experience in performance monitoring, Instance tuning, SQL tuning
- Experience in hot/cold backup mechanisms, EMC BCV concepts
- DBA level experience with UNIX and Linux administration specifically on Linux/Solaris platforms
- Experience in configuring/managing environments with failover/high availability requirements is a plus. Particularly with Standby Databases and Data Guard configuration
- Experience in Security best practices and options

### Education
- Bachelor degree in Engineering/Computer Science or equivalent (must have)
- Oracle Certifications

### 53. Oracle DBA II

#### Responsibilities
- Direct programmers and analysts to make changes to existing databases and database management systems
- Direct others in coding logical and physical database descriptions
- Review project requests describing database user needs to estimate time and cost required to accomplish project
- Review and approve database development and determine project scope and limitations
- Approve, schedule, plan and supervise the installation and testing of new products and improvements to computer systems
- Plan, coordinate, and implement security measures to safeguard information in computer files against accidental or unauthorized damage, modification or disclosure
- Develop standards and guidelines to guide the use and acquisition of software and to

#### Experience
- Strong knowledge of computer software, such as SQL, Visual Basic, Oracle, etc (Required)
- Strong knowledge of computer hardware and software (Required)
- 5+ years hands-on experience with Oracle, with detailed understanding of internals
- Experience with BACKUP/RECOVERY for Oracle databases (must have)
- Experience with Oracle 11gR2, RAC, installation, performance tuning (must have)
- Extremely honed problem-solving and debugging ability (must have)
- Proficiency in BASH scripting (must have) and one of Perl/Python/PHP (nice to have)
- Familiarity with regular expressions for pattern matching and replacement (nice to have)
- Understanding of both OLTP and OLAP concepts (nice to have)
- Understanding of Java, MySQL (nice to have)

#### Education
- Bachelor degree in Engineering/Computer Science or equivalent (must have)
- Oracle Certifications valued, but not required (nice to have)
### 54. Oracle DBA III

#### Responsibilities

Responsible for oversight of multiple stand-alone Oracle database environments. The candidate must have excellent problem management, performance tuning experience and in-depth understanding of Oracle 10g, 11g concepts and best-practice administration standards. The candidate should have project upgrade and transition experience and be able to effectively communicate complex technical topics in summary form to various levels of management and client. The candidate will also participate in critical technical troubleshooting efforts and provide strategic technical advisement as warranted.

- Incident Management including root cause analysis and resolution of high impact/high visibility issues
- Design and execution on significant customer projects
- Mentoring and guidance within overall Oracle technology team
- Participate in internal process and automation improvement opportunities
- Experienced administration of and accountability of multiple stand-alone Oracle databases; including routine administrative activities such as cloning, backup/restore, and patching
- 5+ years of Oracle Database administration experience
- Thorough knowledge of the Oracle RDBMS, architecture, and technology stack

#### Experience

- Broad Oracle product knowledge on existing/new features for customer and senior management roadmap design
- Experience in sizing and architecting large scale environments including RAC based and ASM architecture
- Experience in installation, configuration and support; upgrade of Oracle to latest version
- Experience using Administration, Diagnostic and Tuning capabilities of OEM
- Pro-active management of Production database systems, risks mitigation
- Experience in performance monitoring, Instance tuning, SQL tuning
- Experience in hot/cold backup mechanisms, EMC BCV concepts
- DBA level experience with UNIX and Linux administration specifically on Linux/Solaris platforms
- Instance cloning (RAC, Non-RAC), Code migration processes
- Experience in configuring/managing environments with failover/high availability requirements is a plus. Particularly with Standby Databases and Data Guard configuration
- Experience in Security best practices and options
- Hands on experience in automation as it pertains to monitoring, automated administration, etc.

#### Education

- 4-year degree in MIS/CS or Engineering OR 4+ years of professional work experience
- OCP or relevant certifications preferred
- 8+ years hands-on experience with Oracle Databases.
### Responsibilities

The qualified candidate will have 5 to 10+ years of experience with Oracle EBS including having hands on configuration knowledge. The Oracle EBS Manufacturing Consultant must have strong supporting experience in Manufacturing-related modules commonly implemented as a part of a large-scale Oracle E-Business Suite initiative. An industry background in manufacturing and operational processes is preferred.

- Assume a lead role in the area of Project Suite consulting for Oracle EBS R12
- Expertise in R12 Manufacturing including:
  1. BOM
  2. WIP
  3. Cost Management
  4. MES for Discrete Mfg.
  5. Flow Mfg.
  6. Engineering
  7. Quality
  8. Mobile Supply Chain
  9. Production Scheduling
  10. Manufacturing Scheduling
  11. Manufacturing Operations Center
  12. Oracle Inventory
  13. Process Mfg. and Shop Floor Management is a plus

- Prepare functional requirements for Oracle 11i to R12 upgrades or new R12 implementations
- Provide leadership to functional and development teams and fully participate in all phases of application implementation including requirements planning, functional and technical design, system design and development, testing and deployment support
- Familiarity with SDLC methodology including the standard Oracle AIM approach
- Familiarity with OUM, the recent Oracle Implementation Methodology is a plus
- Provide scoping and estimation input to Practice Executives

### Experience

- 5+ years of hands-on Oracle EBS experience
- Oracle EBS R12 experience at a minimum; Experience with both R12 and 11i functionality a plus
- Expertise in Discrete and Flow Manufacturing Applications.
- Working knowledge of ASCP and WMS applications, as they relate to manufacturing
- Experience with Process Manufacturing Application is a plus
- Experience in creating documentation to support analysis and implementation for all aspects of the E-Business Manufacturing
- Application
- Lead in the planning and execution of testing cycles according to best practices
- Past experience as a team-lead for one or more Oracle 11i/R12 implementations
- Solid understanding of Oracle EBS database/table structures
- Previous manufacturing industry experience is preferred
- Experience with Six Sigma or other Process Improvement methodologies
- Strong communications skills with technical and non-technical users
- Strong written skills including proposal section
### 56. Cyber Security Engineer I

**Education**
Bachelor’s Degree in information technology, computer science, or business management

**Responsibilities**
In this role, the candidate provides comprehensive program management, program control, operations, analysis and administrative support for cyber security policy and information security initiatives.

The job functions are:
- Conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks and remedies.
- Providing recommendations as an authoritative leader in the cyber security, networks, and networks operations arena.
- Determining who requires access to which information, and then plan, coordinate and implement information security programs.
- Designing, architecting, and guiding the technical leadership and recommending solutions to the security problems in the existing systems and the systems under development.

**Experience**
This position requires 2+ years of experience in cyber security, cyber operations, information assurance, information security, technical analysis, or a combination thereof. The experience must include activities such as:
- Gathering, evaluating, and verifying vulnerability for information technology systems, networks, worldwide automated information systems.
- Participating in the development or implementation of information security exercises.
- Monitoring new and emerging information technologies, changes in professional and technical standards and advancements in technology for influence on information security practices.

**Education**
Associate’s Degree: entry-level cyber security specialist positions require a two-year associate’s degree in computer science or a related field.

### 57. Cyber Security Engineer II

**Responsibilities**
In this role, the candidate provides comprehensive program management, program control, operations, analysis and administrative support for cyber security policy and information security initiatives.

The job functions are:
- Conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks and remedies.
- Providing recommendations as an authoritative leader in the cyber security, networks, and networks operations arena.
- Designing, architecting, and guiding the technical leadership and recommending solutions to the security problems in the existing systems and the systems under development.
- Assisting with application of formal methodologies in security architecture, security system design and engineering to help with “security technology” integration and deployment.
### Experience
This position requires 5+ years of experience in cyber security, cyber operations, information assurance, information security, technical analysis, or a combination thereof. The experience must include activities such as:
- Gathering, evaluating, and verifying vulnerability for information technology systems, networks, worldwide automated information systems
- Participating in the development or implementation of information security exercises
- Monitoring new and emerging information technologies, changes in professional and technical standards and advancements in technology for influence on information security practices
- Building and maintaining relationships and partnerships with the stakeholders to exchange security information and promote situational awareness

### Education
Associate’s Degree: entry-level cyber security specialist positions require a two-year associate’s degree in computer science or a related field, plus work experience.

### 58. Cloud Computing Specialist I

#### Responsibilities
In this role, the candidate works with and integrates cloud computing technologies.
- The job functions are:
  - Demonstrating expert-level domain knowledge of VMWARE, VSphere, VCenter, VShield, CITRIX, ZEN, Virtual IDS and cloud management tools
  - Project management and architecting high-visibility cloud computing systems
  - Teaming up with the systems engineers to accomplish project goals
  - Developing and maintaining project plans, schedules and requirements
  - Delivering technical milestones, implementation of the system and on-going support

#### Experience
This position requires:
- Expert-level domain knowledge of VMWARE, VSphere, VCenter, VmWARE VShield, CITRIX, ZEN, Virtual IDS
- Commanding knowledge of "Platform as a Service", "Infrastructure as a Service" and "Software as a Service"
- Planning, coordination, implementation and management of project-related activities
- Help develop roadmaps for proposed solutions
- Produce, maintain and manage requirements, system architecture, and design documents
- Hands-on experience with designing and proto-typing systems and take active role in the development process
- A minimum of 1 or more years of experience in working at data centers or infrastructure engineering projects
- Systems engineering activities including creating requirements definitions, design

#### Education
This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 3 years' experience.
### 59. Cloud Computing Specialist II

**Responsibilities**

In this role, the candidate works with and integrates cloud computing technologies. The job functions are:

- Demonstrating expert-level domain knowledge of VMWARE, VSphere, VCenter, VShield, CITRIX, ZEN, Virtual IDS and cloud management tools
- Project management and architecting high-visibility cloud computing systems
- Teaming up with the systems engineers to accomplish project goals
- Developing and maintaining project plans, schedules and requirements
- Delivering technical milestones, implementation of the system and on-going support

**Experience**

This position requires:

- Expert-level domain knowledge of VMWARE, VSphere, VCenter, VmWARE VShield, CITRIX, ZEN, Virtual IDS
- Commanding knowledge of "Platform as a Service", "Infrastructure as a Service" and "Software as a Service"
- Planning, coordination, implementation and management of project-related activities
- Help develop roadmaps for proposed solutions
- Produce, maintain and manage requirements, system architecture, and design documents
- Hands-on experience with designing and proto-typing systems and take active role in the development process
- A minimum of 3 or more years of experience in working at data centers or infrastructure engineering projects
- Systems engineering activities including creating requirements definitions, design documents and implementation
- Must have at least 5+ years of experience as a Cloud Computing Specialist

**Education**

This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 5 years' experience.

### 60. Cloud Computing Specialist III

**Responsibilities**

In this role, the candidate works with and integrates cloud computing technologies. The job functions are:

- Demonstrating expert-level domain knowledge of VMWARE, VSphere, VCenter, VShield, CITRIX, ZEN, Virtual IDS and cloud management tools
- Project management and architecting high-visibility cloud computing systems
- Teaming up with the systems engineers to accomplish project goals
- Developing and maintaining project plans, schedules and requirements
- Delivering technical milestones, implementation of the system and on-going support
**Experience**

This position requires:

- expert-level domain knowledge of VMWARE, VSphere, VCenter, VmWARE VShield, CITRIX, ZEN, Virtual IDS
- commanding knowledge of "Platform as a Service", "Infrastructure as a Service" and "Software as a Service"
- planning, coordination, implementation and management of project-related activities
- help develop roadmaps for proposed solutions
- produce, maintain and manage requirements, system architecture, and design documents
- hands-on experience with designing and proto-typing systems and take active role in the development process
- a minimum of 5 or more years of experience in working at data centers or infrastructure engineering projects
- systems engineering activities including creating requirements definitions, design documents and implementation
- Must have at least 3+ years of experience
- Must have at least 7+ years of experience as a Cloud Computing Specialist and 3+ years of

**Education**

This position requires a minimum of a baccalaureate degree or higher in related field with a minimum of 8 years' experience.

---

**61. Systems Administrator I**

**Responsibilities**

- Perform basic systems security administration functions, including creating customer profiles and accounts
- Monitor and manages system resources, including CPU usage, disk usage, and response times to maintain operating efficiency
- Write or modify basic scripts to resolve performance problems and automate systems administration tasks
- Maintain system documentation and logs
- Perform or assist in troubleshooting and diagnosing production problems; corrects identified problems
- Perform systems administration functions for the District wide e-mail system
- Maintain application security, event investigations and compliance enforcement.
- Monitor and manages system resources, including CPU usage, disk usage, and response times to maintain operating efficiency
- Account Management

**Experience**

- One year of increasingly responsible experience in computer applications programming and systems analysis
- Demonstrated competency in systems documentation
- Concept and administration of computer and network operating systems and applications.
- Practice and methods of systems administration and maintenance
- Network protocols including TCP/IP and bridging
- Data storage and communications
- Principles, practices, and techniques in the installation, maintenance and troubleshooting of server hardware and software
- Reporting tools, Excel, Crystal Reports, etc.
<table>
<thead>
<tr>
<th>Education</th>
<th>Equivalent to a bachelor’s degree from an accredited college or university with major course work in Computer Science, Management Information Systems, or a closely related field</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>62. Systems Administrator II</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Responsibilities** | ● Maintain system documentation and logs  
● Perform systems administration functions for the District wide e-mail system  
● Maintain application security, event investigations and compliance enforcement.  
● Administer secure links with public key encryption, anti-virus, user authentication and intrusion detection  
● Provide monitoring and primary response and intervention for information technology related security incidents and violations  
● Keep current with new Information Technology Security protocols, applicable laws and regulations  
● Management of Active Directory  
● Management of users and computers  
● Management of access to resources, computer environment etc.  
● Monitoring network access  
● Thorough understanding of TCP/IP, different protocols and OSI Model  
● Quickly arrange repair for hardware in occasion of hardware failure  
● Implement the policies for the use of the computer system and network  
● Setup security policies for users. A system admin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems). |
| **Experience** | ● Two years of increasingly responsible computer applications programming and systems analysis experience  
● A minimum of two years progressive experience in various Information Technology related functions including but not limited to information server standard administration  
● Strong operating system and network knowledge in order to carry out assigned administrative tasks with the need for limited supervision  
● Overall system administration responsibility for major platform and operating systems  
● Local Area Networks (LANs) and Wide Area Networks (WANs)  
● Reporting tools, Excel, Crystal Reports, etc. |
| **Education** | A bachelor’s degree from an accredited college or university with major course work in Computer Science, Management Information Systems, or a closely related field |
### 63. Hyperion Functional Analyst III

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Act as the Subject matter Expert for Hyperion Reporting, Planning, HFM and or Cognos BI projects supporting finance business initiatives including plan development, status, resource planning.</td>
<td></td>
</tr>
<tr>
<td>Work with internal departments to enhance the use and functionality within the Oracle and Hyperion Suite of products to its fullest extent.</td>
<td></td>
</tr>
<tr>
<td>Write and develop reports to extract data out of existing business systems utilizing system functionality.</td>
<td></td>
</tr>
<tr>
<td>Collaborate with IT on technical change/enhancements specifications that will be used to drive change in the organization.</td>
<td></td>
</tr>
<tr>
<td>Provide 1st level support and training in the area of finance to troubleshoot issues within Hyperion and Oracle ERP Suite implemented across ADP and escalation to Division IT team when needed.</td>
<td></td>
</tr>
<tr>
<td>Document and manage the flow of enhancements for various Hyperion enhancements with the IT Department and key Finance stakeholders.</td>
<td></td>
</tr>
<tr>
<td>Understand, document, implement, and certify that processes to support interfacing to internal &amp; 3rd party tools in the area of finance.</td>
<td></td>
</tr>
<tr>
<td>Understand and document opportunities for business efficiencies within an assigned business operation.</td>
<td></td>
</tr>
<tr>
<td>Ensure that documentation, procedures and processes are compliant with SOX &amp; GAAP requirements.</td>
<td></td>
</tr>
<tr>
<td>Research, define, document, and deploy business processes within Global Finance Operations as required by ADP.</td>
<td></td>
</tr>
<tr>
<td>Research tools and applications within Hyperion, Oracle EBS to maximize use across all areas.</td>
<td></td>
</tr>
<tr>
<td>Lead the implementation of business processes, applications, and IT tools within ADP organizations including testing, documentation, and user training.</td>
<td></td>
</tr>
<tr>
<td>Analyze, design and impact assessment of business and configuration changes including data and metadata management on available business model</td>
<td></td>
</tr>
<tr>
<td>Support continuous application process optimizations</td>
<td></td>
</tr>
<tr>
<td>Meet service commitments for assigned deliverables and proactively provide work status</td>
<td></td>
</tr>
<tr>
<td>Organize and prepare work effectively to facilitate proactive resolution of problems, rather than reactive</td>
<td></td>
</tr>
<tr>
<td>Anticipate, identify, track and resolve issues and risks affecting the application</td>
<td></td>
</tr>
<tr>
<td>Coordinates month end closure and also be able to handle reconciliations</td>
<td></td>
</tr>
</tbody>
</table>
| Experience | • Overall technical understanding of one or more Hyperion system 9.x.x EPM suite (Essbase and HFM) components.  
• Essbase optimization knowledge  
• Strong written and oral communication skills and presentation skills.  
• Strong analytical skills, problem recognition and problem solving / issue resolution skills along with coordination skills.  
• Expertise in detailed requirements gathering and documentation of requirements, including requirements for functional design.  
• Expertise in Testing and creating Requirements Traceability matrix.  
• Expertise in Enterprise Life Cycle processes and Managed Services mode  
• Experience with and establishing financial/ business processes and implementing IS tools to support internal & 3rd party solutions in the area of finance  
• Proven experience in support of SOX & GAAP practices in a services environment  
• Hands-on experience working with Hyperion EPM / Oracle Applications (FDM/EPMA) - in the area of Accounting and Finance is required  
• Experience with data modeling, profiling, and reporting cubes is a plus  
• Experience with other BI tools like Hyperion Planning, Hyperion Reporting, Cognos is a plus  
• Experience with Oracle GL and/or other EBS Modules is a plus  
• Strong communication skills  
| Education | 4 year degree in finance, accounting, computer science or related degree and appropriate experience  
• Minimum 5 years’ experience supporting developing/evaluating HFM applications from a functional / end user prospective supporting a finance organization  
| Responsibilities | • Ensure timely flow of consistent, accurate financial and operating information using the Essbase tool and SAP  
• Support tactical and strategic development initiatives for management reporting, data warehousing and profitability reporting  
• Update the business rules and logic in Essbase-based calculations for yearly business rules for Budgets, Forecasts and Profitability  
• Partner with Business Controllers and the Finance technology team to develop and roll out new Essbase cubes and reporting solutions for the Finance organization  
• Enhance business and technical processes by clarifying/defining business processes, identifying opportunities for automation and/or technical solutions and working with the technology teams on the implementation  
• Facilitate the monthly business cycles by performing required system maintenance  
• Performance tuning as well as high availability and clustering.  |
| **Experience** | At least 5 years of experience working with Hyperion Essbase and related tools  
|               | A good understanding of Finance/Accounting data structures and data management practices with the ability to communicate clearly on that topic.  
|               | Strong understanding of basic General Ledger systems and Data Warehousing systems  
|               | Advanced proficiency in all MS Office applications (special emphasis on advanced functions of Excel)  
|               | Experience using Spotfire Cognos or other BI tools is desirable; SAP experience a strong plus  
|               | Financial Services industry knowledge is a plus  
|               | Experience in VB scripting, Essbase calc scripts desirable  
|               | Experience in Technical infrastructure experience for Hyperion applications  
|               | Experience in Architecture/ installation experience for Hyperion w/ ERP integration and Hyperion w/ OBIEE integration  
|               | Experience in ETL skills: SQL, DIM/Informatica, Oracle Data Integrator (ODI)  
|               | Experience in Scripting skills: MAXL, Esscmd, Perl, Unix Scripting, Windows Batch  
|               | Experience in Application Server skills: J2EE, WebLogic, Tomcat, WebSphere  
|               | Good understanding of LDAP/MSAD, LAN/WAN and SAN/ NAS technologies  
|               | Good understanding of virtualization technologies  
|               | Good understanding of relational technologies: SQL Server, Oracle  
|               | Experience leading technical teams (developers and infrastructure architects/analysts)  
|               | Must have exceptional Hyperion architecture, installation and troubleshooting skills with a strong technical background.  
|               | Must have solid infrastructure background and expertise specific to Oracle Hyperion application installations, integration with existing infrastructure, Microsoft Active Directory/LDAP authentication configuration for Hyperion,  
|               | Experience architecting and building Production and Development environments for Oracle’s EPM 11 Suite consisting of Hyperion Planning, HFM, Essbase, EAS, Financial Reporting, FDM, EAL, EPMA and HSF.  
|               | Ability to work effectively both independently and in groups and in project roles and environments  
|               | Excellent problem-solving and communication skills |

| **Education** | A Bachelor’s Degree required, Accounting or Finance major preferred |
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 Information Technology Schedule.

   b. Services under this SIN are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers 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: 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 - (not all vendors have been placed within the following subcategories. To view a complete list of vendors, click on the SIN)

   - 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 sub-category 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 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 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
A description of the labor categories offered under this SIN begin on page 67 of this pricelist.
# LABOR DESCRIPTIONS (54151HACS)

## High Value Asset Assessments

<table>
<thead>
<tr>
<th>Cybersecurity SME</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Analyst I</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Analyst II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
</tbody>
</table>
information systems from an accredited college or university or equivalent work experience.

<table>
<thead>
<tr>
<th>Cybersecurity Analyst III</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Reviews and provides recommendations for security assessment plans and results. Creates plans of action and milestones (POA&amp;Ms). Prepares and documents findings. Assists with the assessment and authorization process. Assists the engineer at times with conducting system analysis, design, development, test and evaluation activities, ensuring the integration of software, hardware, reliability, maintainability, safety, survivability, human and other requirements in the total security engineering effort. Identifies requirements and participates in information analysis, cost-benefit analysis, system trade studies and risk analysis. Assists in the selection of system architecture components, allocating requirements and preparing specifications.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
<td>At least 7 years of experience.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Architect I</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Develops and recommends technical solutions to support client’s requirements for solving network, platform and system security problems. Typical focus areas include analytical and engineering solutions based on federal and industry INFOSEC policy, doctrine and regulations. Supports secure system engineering and development, including system/security requirements analysis, secure system definition and specification, and development of INFOSEC policies and procedures, utilizing technical and analytical skills. Also helps design test beds for the DT&amp;E of advanced INFOSEC hardware and software solutions.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
<td>At least 5 years of experience with at least 2 years of specialized experience in defining high-level security requirements.</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cybersecurity Architect II</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Provides customer support in solving all phases of complex INFOSEC-related technical problems. Reviews and recommends INFOSEC solutions to customer problems based on an understanding of product/system test results and a firm understanding of government/industry policy, practices, procedures and customer requirements. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration, and testing of INFOSEC products and techniques. Gives particular attention to Guard, Firewall, Secure Network Server, “Smart Cards,” emerging security technologies and future trends in support of information system and network security. Ensures that INFOSEC solutions are fully compatible with or engineered into the customer’s network design. Provides work direction and guidance to other personnel; ensures accuracy of the work of other personnel. Operates under deadlines and is able to work on multiple tasks. Frequently leads teams or small groups of personnel in performing complex security-related tasks.</td>
</tr>
<tr>
<td><strong>Experience</strong></td>
<td>At least 7 years of experience with at least 4 years of specialized experience in defining high-level security requirements.</td>
</tr>
</tbody>
</table>
**Cybersecurity Architect III**

| **Description** | Provides customer support in solving all phases of complex INFOSEC-related technical problems. Reviews and recommends INFOSEC solutions to customer problems based on an understanding of product/system test results and a firm understanding of government/industry policy, practices, procedures and customer requirements. Conducts systems security analysis and implementation, system engineering, electrical design, design assurance, testing, software engineering, program design, configuration management, integration, and testing of INFOSEC products and techniques. Gives particular attention to Guard, Firewall, Secure Network Server, “Smart Cards,” emerging security technologies and future trends in support of information system and network security. Ensures that INFOSEC solutions are fully compatible with or engineered into the customer’s network design. Provides daily supervision and direction to staff; ensures accuracy of the work of other personnel. Operates under deadlines and is able to work on multiple tasks. Anticipates future customer, industry, and business trends, information and situations and implements related actions independently or through the management team. |
| **Experience** | At least 9 years of experience with at least 6 years of specialized experience in defining high-level security requirements. |
| **Education** | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |

**Cybersecurity System Engineer I**

| **Description** | Receives assignments in the form of objectives and establishes goals to meet those objectives on schedule. Performs engineering activities that include defining system requirements, developing technical solutions, performing systems functional analysis, conducting trade studies and performing test and evaluation activities. Works on problems where analysis of data requires an evaluation of various factors. Exercises independent judgment within broadly defined area. Contributes to the development of organization’s goals and objectives. Ensures project schedules and performance requirements are met. Frequently interacts with customers and functional peer groups, gaining cooperation of others, overseeing production and maintaining work schedules. |
| **Experience** | At least 2 years of experience. |
| **Education** | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |

**Cybersecurity System Engineer II**

<p>| <strong>Description</strong> | Receives assignments in the form of objectives and establishes goals to meet those objectives on schedule. Performs engineering activities that include defining system requirements, developing technical solutions, performing systems functional analysis, conducting trade studies and performing test and evaluation activities. Works on problems where analysis of data requires an evaluation of various factors. Exercises independent judgment within broadly defined area. Contributes to the development of organization’s goals and objectives. Ensures project schedules and performance requirements are met. Frequently interacts with customers and functional peer groups, gaining cooperation of others, overseeing production and maintaining work schedules. |
| <strong>Experience</strong> | At least 2 years of experience. |
| <strong>Education</strong> | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |</p>
<table>
<thead>
<tr>
<th>Role</th>
<th>Experience</th>
<th>Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity System Engineer III</td>
<td>At least 4 years of experience.</td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
<tr>
<td>Cybersecurity Application Engineer I</td>
<td>At least 2 years of experience.</td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
<tr>
<td>Cybersecurity Application Engineer II</td>
<td>At least 4 years of experience.</td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
<tr>
<td>Cybersecurity Application Engineer III</td>
<td>At least 7 years of experience.</td>
<td>This position requires a minimum of a master’s degree in computer science or information systems from an accredited college or university or equivalent work experience.</td>
</tr>
<tr>
<td>Experience</td>
<td>At least 6 years of experience.</td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
<td></td>
</tr>
</tbody>
</table>

**Cybersecurity Cloud Engineer I**

| Description | Leads and/or performs the custom design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingestion, acceptance testing, management and operations/maintenance/enhancements to deploy virtualization/cloud computing capabilities in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize commercial-off-the-shelf (COTS) technologies into the larger software solution. Leverages Web Services and/or APIs. Ensures the cloud solution is free of common or known security vulnerabilities. Communicates proficiently in various technology collaboration tools. Reports system performance through visualization dashboards. Creates and updates associated technical documentation and user manuals consistent with prevailing governance framework. Diagnoses performance issues and outages and provides associated communications and After-Action Reports. Identifies and recommends process enhancements. Engages cloud providers. Engages customer’s technical product managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower-level engineers. |
| Experience | At least 2 years of experience. |
| Education  | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |

**Cybersecurity Cloud Engineer II**

| Description | Leads and/or performs the custom architecture, design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingestion, acceptance testing, management and operations/maintenance/enhancements to deploy advanced virtualization/cloud computing capabilities in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize commercial-off-the-shelf (COTS) technologies into the larger software solution. Builds, designs and leverages Web Services and/or APIs. Ensures the cloud solution is free of common or known security vulnerabilities. Communicates proficiently in various technology collaboration tools. Reports system performance through visualization dashboards. Creates and updates associated technical documentation and user manuals consistent with prevailing governance framework. Diagnoses advanced performance issues and outages and provides associated communications and After-Action Reports. Identifies and recommends process enhancements. Engages cloud providers. Engages customer’s technical product managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower-level engineers. |
| Experience | At least 4 years of experience. |
| Education  | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |
### Cybersecurity Cloud Engineer III

**Description**  
Leads and/or performs the custom architecture, design, planning, implementation, orchestration/automation, troubleshooting, quality testing, data ingestion, acceptance testing, management and operations/maintenance/enhancements to deploy complex virtualization/cloud computing capabilities in accordance with customer-specified requirements and platform environments. May also be required to integrate, adapt/customize and optimize commercial-off-the-shelf (COTS) technologies into the larger software solution. Builds, designs and leverages Web Services and/or APIs. Ensures the cloud solution is free of common or known security vulnerabilities. Communicates expertly in various technology collaboration tools. Reports system performance through visualization dashboards. Creates and updates associated technical documentation and user manuals consistent with prevailing governance framework. Diagnoses unique or complex performance issues and outages and provides associated communications and After-Action Reports. Identifies and recommends process enhancements. Engages cloud providers. Engages customer’s technical product managers and other engineers as necessary throughout the engineering activities. May provide supervisory guidance to lower-level engineers.

**Experience**  
At least 8 years of experience.

**Education**  
This position requires a minimum of a master’s degree in computer science or information systems from an accredited college or university or equivalent work experience.

---

### Risk and Vulnerability Assessment

#### Vulnerability Analyst I

**Description**  
Possesses a working knowledge of database security; vulnerability testing; networking protocols and topologies; security architectures; incident management; and network technologies, such as Windows and Linux operating systems, Active Directory, and service-oriented architectures (SOAs). Also has experience conducting web application, operating system, database and wireless testing and assessments using COTS tools. Develops technical solutions for information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools and data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, identify, contain, and eradicate intrusions and intrusion attempts. Ensures required cybersecurity policies are adhered to and that required controls are implemented. Supports program lead with detection, assessment, communication, and coordination of the remediation of security vulnerabilities. Supports engineers in troubleshooting and gathering data required to perform remediation to maintain an acceptable security posture. Analyzes vulnerability reports to ensure data accuracy, provide technical vulnerability analysis and determine remediation options. Provides metrics and reporting on changes to the state of system security, threat, vulnerability and patch management. Monitors public and proprietary sources for vulnerability information. Maintains and composes operational process documentation regarding program execution.

**Experience**  
At least 2 years of experience.

**Education**  
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.

---

#### Vulnerability Analyst II

**Description**  
Possesses a working knowledge of database security; vulnerability testing; networking...
protocols and topologies; security architectures; incident management; and network
technologies, such as Windows and Linux operating systems, Active Directory, and service-
oriented architectures (SOAs). Also has experience conducting web application, operating
system, database and wireless testing and assessments using COTS tools. Develops technical
solutions for information operations and analysis related to security intrusion analysis,
systems and vulnerabilities, network security, advanced analytic tools and data visualization
techniques. Serves as lead analyst in the detection of malicious activity to prevent, identify,
contain, and eradicate intrusions and intrusion attempts. Conducts analysis of system logs,
forensic results, vulnerability assessment tool results, and risks, and investigates instances of
security concern throughout the enterprise. Ensures required cybersecurity policies are
adhered to and that required controls are implemented. Supports program lead with detection,
assessment, communication, and coordination of the remediation of security vulnerabilities.
Supports engineers in troubleshooting and gathering data required to perform remediation to
maintain an acceptable security posture. Analyzes vulnerability reports to ensure data
accuracy, provide technical vulnerability analysis and determine remediation options.
Provides metrics and reporting on changes to the state of system security, threat, vulnerability
and patch management. Monitors public and proprietary sources for vulnerability
information. Maintains and composes operational process documentation regarding program
execution.

| Experience | At least 4 years of experience. |
| Education | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |

<table>
<thead>
<tr>
<th>Vulnerability Analyst III</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Possesses a working knowledge of database security; vulnerability testing; networking protocols and topologies; security architectures; incident management; and network technologies, such as Windows and Linux operating systems, Active Directory, and service-oriented architectures (SOAs). Also has experience conducting web application, operating system, database and wireless testing and assessments using COTS tools. Develops technical solutions for information operations and analysis related to security intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools and data visualization techniques. Serves as lead analyst in the detection of malicious activity to prevent, identify, contain, and eradicate intrusions and intrusion attempts. Conducts analysis of system logs, forensic results, vulnerability assessment tool results, and risks, and investigates instances of security concern throughout the enterprise. Ensures required cybersecurity policies are adhered to and that required controls are implemented. Supports program lead with detection, assessment, communication, and coordination of the remediation of security vulnerabilities. Supports engineers in troubleshooting and gathering data required to perform remediation to maintain an acceptable security posture. Analyzes vulnerability reports to ensure data accuracy, provide technical vulnerability analysis and determine remediation options. Provides metrics and reporting on changes to the state of system security, threat, vulnerability and patch management. Monitors public and proprietary sources for vulnerability information. Maintains and composes operational process documentation regarding program execution.</td>
<td></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
<td>At least 8 years of experience.</td>
<td></td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.</td>
<td></td>
</tr>
</tbody>
</table>
### Cyber Security Threat Analyst I

| Description | Collects intelligence, including Indicators of Compromise (IoCs). Develops and maintains specialized knowledge related to crimeware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and distributed denial of service (DDOS) techniques. 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 makes 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 written and/or presentation form to stakeholders/customers. Supports studies to identify cyber threats, threat vectors, threat actors and threat trends. Counters the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Identifies threat signatures from available sources. Performs cyber incident triage, including determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation. Supports standard procedures for incident response. Interfaces with Security Officers and Incident Response Teams. Working knowledge of technical security countermeasures systems and regulations regarding technical, physical and procedural security is desired. |
| Experience | At least 2 years of experience. |
| Education | This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience. |

### Cyber Security Threat Analyst II

| Description | Collects intelligence, including Indicators of Compromise (IoCs). Develops and maintains specialized knowledge related to crimeware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and distributed denial of service (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 makes 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 written and/or presentation form to stakeholders/customers. Conducts studies and makes recommendations to identify cyber threats, threat vectors, threat actors and threat trends. Counters the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Identifies and develops threat signatures from available sources. Performs cyber incident triage, including determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation. Maintains threat indicators in a threat intelligence platform. Implements and supports standard procedures for incident response. Interfaces with Security Officers and Incident Response Teams. Possesses knowledge and understanding of intelligence community standards and directives. Working knowledge of technical security countermeasures systems |

74
Cybersecurity Threat Analyst III

Description
Leads teams and/or projects in collecting intelligence, including Indicators of Compromise (IoCs). Develops and maintains specialized knowledge related to crimeware, botnets, state-affiliated actors, high-level organized crime, hacktivism, and distributed denial of service (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 makes 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 written and/or presentation form to stakeholders/customers. Conducts studies and makes recommendations to identify cyber threats, threat vectors, threat actors and threat trends. Counters the threat posed by foreign cyber actors against information systems, critical infrastructure and cyber-related interests. Identifies and develops threat signatures from available sources. Performs cyber incident triage, including determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation. 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 in internal and external threat intelligence and cybersecurity forums. Communicates with stakeholders and other team/project leaders. Possesses knowledge and understanding of intelligence community standards and directives. Working knowledge of technical security countermeasures systems and regulations regarding technical, physical and procedural security is desired.

Experience
At least 6 years of experience.

Education
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.

Incident Response

Incident Response Analyst I

Description
Contributes to response to crisis or urgent situations to mitigate immediate and/or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Handles and responds to cybersecurity incidents through coordination with stakeholders, such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement and privacy offices. Intakes incident reporting, conducts ticket updates and notifies stakeholders of cybersecurity incidents and forensic investigations related to computer security incidents, escalating when necessary as well as coordinating response to computer security incidents. Recommends a course of action on each incident and creates, manages and records all actions taken. Serves as initial point of contact (POC) for Events of Interest reported both internally and externally. Establishes alarm/incident escalation process and tracks, follows up on, and resolves incidents. Initiates and maintains contact with affected parties during incident...
<table>
<thead>
<tr>
<th>Incident Response Analyst II</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Response Analyst III</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Experience</strong></td>
</tr>
<tr>
<td><strong>Education</strong></td>
</tr>
</tbody>
</table>
### Incident Response Forensic Analyst I

**Description**
Actively leads or participates in critical incident response functions. Works with standard forensics tools (e.g., EnCase) at a high level of technical proficiency. Communicates effectively with managers and individual contributors during an incident response situation. Improves processes for incident response, threat hunting, content development and data enrichment. Fosters communication between security groups and serves as the center point of contact for escalation on a multitude of issues.

**Experience**
At least 2 years of experience.

**Education**
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.

### Incident Response Forensic Analyst II

**Description**
Actively leads or participates in critical incident response functions. Works with standard forensics tools (e.g., EnCase) at a high level of technical proficiency. Communicates effectively with managers and individual contributors during an incident response situation. Improves the processes for incident response, threat hunting, content development, and data enrichment. Fosters communication between security groups and serves as the center point of contact for escalation on a multitude of issues.

**Experience**
At least 6 years of experience.

**Education**
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.

### Penetration Testing

#### Penetration Tester I

**Description**
Conducts and/or supports authorized penetration testing on enterprise network assets. Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems. Analyzes site/enterprise defensive cyber operations (DCO) policies and configurations and evaluates compliance with regulations and enterprise directives. Assists with the selection of cost-effective security controls to mitigate risk. Assesses threats to the environment via penetration testing, risk assessments and other assessments. Provides inputs on the adequacy of security designs and architectures. Supports cybersecurity assessments and defensive and offensive operations. Provides support for security certification test and evaluation of assets, vulnerability management and response, and security assessments. Provides customer support and guidance.

**Experience**
At least 2 years of experience.

**Education**
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.

#### Penetration Tester II

**Description**
Conducts and/or supports authorized penetration testing on enterprise network assets. Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems. Analyzes site/enterprise defensive cyber operations (DCO) policies and configurations and evaluates compliance with regulations and enterprise directives. Assists with the selection of cost-
Conducts and/or supports authorized penetration testing on enterprise network assets. Emulates adversarial cyber activities to identify weaknesses, enumerate vulnerabilities, and assess the overall security posture of customer networks and information systems. Analyzes site/enterprise defensive cyber operations (DCO) policies and configurations and evaluates compliance with regulations and enterprise directives. Assists with the selection of cost-effective security controls to mitigate risk. Assesses threats to the environment via penetration testing, risk assessments and other assessments. Provides inputs on the adequacy of security designs and architectures. Supports cybersecurity assessments and defensive and offensive operations. Provides support for security certification test and evaluation of assets, vulnerability management and response, and security assessments. Provides customer support and guidance.

Experience
At least 7 years of experience.

Education
This position requires a minimum of a bachelor’s degree or higher in computer science or information systems from an accredited college or university or equivalent work experience.
# PRICE LIST TO GSA

<table>
<thead>
<tr>
<th>SIN</th>
<th>LABOR CATEGORY</th>
<th>Unit of Issue</th>
<th>Price Offered to GSA (including IFF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151S</td>
<td>Business Intelligence Analyst II</td>
<td>Hour</td>
<td>$136.35</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Intelligence Analyst III</td>
<td>Hour</td>
<td>$161.26</td>
</tr>
<tr>
<td>54151S</td>
<td>Business Intelligence SME</td>
<td>Hour</td>
<td>$161.26</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Analyst I</td>
<td>Hour</td>
<td>$92.85</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Analyst II</td>
<td>Hour</td>
<td>$99.00</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Analyst III</td>
<td>Hour</td>
<td>$107.51</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Security Analyst I</td>
<td>Hour</td>
<td>$99.00</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Security Analyst II</td>
<td>Hour</td>
<td>$100.18</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Security SME</td>
<td>Hour</td>
<td>$128.35</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Systems Security Officer (ISSO)</td>
<td>Hour</td>
<td>$140.93</td>
</tr>
<tr>
<td>54151S</td>
<td>Information Security Analyst III (CYBER SECURITY)</td>
<td>Hour</td>
<td>$124.61</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Engineer I</td>
<td>Hour</td>
<td>$95.78</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Engineer II</td>
<td>Hour</td>
<td>$112.88</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Security Engineer III</td>
<td>Hour</td>
<td>$136.83</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer II</td>
<td>Hour</td>
<td>$98.03</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer III</td>
<td>Hour</td>
<td>$136.83</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing Specialist I</td>
<td>Hour</td>
<td>$98.47</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing Specialist II</td>
<td>Hour</td>
<td>$103.72</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing Specialist III</td>
<td>Hour</td>
<td>$107.51</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing Lead &amp; Project Manager</td>
<td>Hour</td>
<td>$149.52</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing SME</td>
<td>Hour</td>
<td>$149.52</td>
</tr>
<tr>
<td>54151S</td>
<td>Cloud Computing Architect</td>
<td>Hour</td>
<td>$166.10</td>
</tr>
<tr>
<td>54151S</td>
<td>Cyber Security Engineer I</td>
<td>Hour</td>
<td>$100.18</td>
</tr>
<tr>
<td>54151S</td>
<td>Cyber Security Engineer II</td>
<td>Hour</td>
<td>$112.88</td>
</tr>
<tr>
<td>54151S</td>
<td>Cyber Security Architect</td>
<td>Hour</td>
<td>$161.26</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle Application Developer (Technical) II</td>
<td>Hour</td>
<td>$108.17</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle Application Developer (Technical) III</td>
<td>Hour</td>
<td>$161.26</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle DBA I</td>
<td>Hour</td>
<td>$97.73</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle DBA II</td>
<td>Hour</td>
<td>$98.47</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle DBA III</td>
<td>Hour</td>
<td>$103.72</td>
</tr>
<tr>
<td>54151S</td>
<td>Oracle Functional Consultant III</td>
<td>Hour</td>
<td>$146.60</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Administrator I</td>
<td>Hour</td>
<td>$63.53</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Administrator II</td>
<td>Hour</td>
<td>$109.46</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer I</td>
<td>Hour</td>
<td>$92.82</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer II</td>
<td>Hour</td>
<td>$97.50</td>
</tr>
<tr>
<td>Code</td>
<td>Position</td>
<td>Rate</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Hyperion Functional Analyst III</td>
<td>Hour $161.26</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Hyperion Technical Specialist III</td>
<td>Hour $161.26</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Writer I</td>
<td>Hour $63.53</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Writer II</td>
<td>Hour $93.50</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Writer III</td>
<td>Hour $98.00</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Certification &amp; Accreditation Specialist</td>
<td>Hour $99.00</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Technical Lead and Project Manager</td>
<td>Hour $124.61</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Cyber Security Lead and Project Manager</td>
<td>Hour $133.73</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Help Desk Support Service Specialist II</td>
<td>Hour $109.95</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Help Desk Support Service Specialist III</td>
<td>Hour $128.35</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Windows System Engineering SME</td>
<td>Hour $133.73</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Web and Intranet Applications Specialist II</td>
<td>Hour $119.23</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software Developer</td>
<td>Hour $92.85</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software Developer II</td>
<td>Hour $103.72</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer II</td>
<td>Hour $106.79</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software Engineer III</td>
<td>Hour $113.30</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Web Designer I</td>
<td>Hour $82.88</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Web Designer II</td>
<td>Hour $92.82</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Web Application Developer I</td>
<td>Hour $101.00</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Web Application Developer II</td>
<td>Hour $107.51</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Database Application Developer II</td>
<td>Hour $95.78</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software QA Analyst I</td>
<td>Hour $92.70</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software QA Analyst II</td>
<td>Hour $97.50</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Software QA Analyst III</td>
<td>Hour $98.47</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Database Administrator I</td>
<td>Hour $95.00</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Database Administrator II</td>
<td>Hour $95.51</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager I</td>
<td>Hour $92.70</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager II</td>
<td>Hour $97.00</td>
<td></td>
</tr>
<tr>
<td>54151S</td>
<td>Senior Project Manager</td>
<td>Hour $112.88</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security SME</td>
<td>Hour $148.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst I</td>
<td>Hour $118.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst II</td>
<td>Hour $129.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Analyst III</td>
<td>Hour $142.78</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Architect I</td>
<td>Hour $128.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Architect II</td>
<td>Hour $140.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Architect III</td>
<td>Hour $154.88</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security System Engineer I</td>
<td>Hour $126.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security System Engineer II</td>
<td>Hour $138.60</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security System Engineer III</td>
<td>Hour $152.46</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Application Engineer I</td>
<td>Hour $131.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Application Engineer II</td>
<td>Hour $144.10</td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Job Title</td>
<td>Rate</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Application Engineer III</td>
<td>$158.51</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Cloud Engineer I</td>
<td>$135.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Cloud Engineer II</td>
<td>$148.50</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Cloud Engineer III</td>
<td>$163.35</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Vulnerability Analyst I</td>
<td>$118.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Vulnerability Analyst II</td>
<td>$129.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Vulnerability Analyst III</td>
<td>$142.78</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Threat Analyst I</td>
<td>$128.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Threat Analyst II</td>
<td>$140.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Threat Analyst III</td>
<td>$154.88</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Analyst I</td>
<td>$118.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Analyst II</td>
<td>$129.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Analyst III</td>
<td>$142.78</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Forensic Analyst I</td>
<td>$138.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Incident Response Forensic Analyst II</td>
<td>$151.80</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester I</td>
<td>$126.00</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester II</td>
<td>$138.60</td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Penetration Tester III</td>
<td>$152.46</td>
<td></td>
</tr>
</tbody>
</table>