GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE

AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICELIST

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

Multiple Award Schedule (MAS)
Information Technology Category

Contract Number: GS-35F-0398V

CollabraLink Technologies, Inc.
8405 Greensboro Drive, Suite 600
McLean, VA 22102
Phone: (703) 639-1780
Fax: (703) 639-1787
www.collabralink.com

Business Size / Status: Other than Small Business
Period Covered by Contract: 05/01/2009 - 04/30/2024
Pricelist current through PS-0030, dated July 8, 2022

For more information on ordering from Federal Supply Schedules go to the GSA Schedules page at GSA.gov. Prices shown herein are net (discount deducted)
Special Item Number 518210C, Cloud and Cloud-Related IT Professional Services
Special Item Number 54151HACS, Highly Adaptive Cybersecurity Solutions (HACS)
Special Item Number 54151HEAL, Health Information Technology Services
Special Item Number 54151S, Information Technology Professional Services

FPDS Code D301  IT Facility Operation and Maintenance
FPDS Code D302  IT Systems Development Services
FPDS Code D306  IT Systems Analysis Services
FPDS Code D307  Automated Information Systems Design and Integration Services
FPDS Code D308  Programming Services
FPDS Code D310  IT Backup and Security Services
FPDS Code D311  IT Data Conversion Services
FPDS Code D316  IT Network Management Services
FPDS Code D317  Creation/Retrieval of IT Related Automated News Services, Data Services, or Other Information Services (All other information services belong under Schedule 76)
FPDS Code D399  Other Information Technology Services, Not Elsewhere Classified

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

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

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

Special Item Number OLM, Order Level Materials

518210C STLOC, 54151HACS STLOC, 54151HEAL STLOC, 54151S STLOC, OLM STLOC: Section 211 of the E-Government Act of 2002 (the Act) amended the Federal Property and Administrative Services Act to allow for “Cooperative Purchasing.” Cooperative Purchasing allows for the Administrator of General Services to provide states and localities access to certain categories offered through the General Services Administration’s Multiple Award Schedule contract. The information technology available to state and local governments includes automated data processing equipment (including firmware), software, supplies, support equipment, and services.

518210C RC, 54151HACS RC, 54151HEAL RC, 54151S RC, OLM RC: Section 833 of the National Defense Authorization Act allows state and local governments to purchase products and services to facilitate recovery from a major disaster. This includes advance and pre-positioning in preparation for a disaster.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CUSTOMER INFORMATION</td>
<td>1</td>
</tr>
<tr>
<td>GSA CLOUD IT PROFESSIONAL SERVICES LABOR CATEGORIES - SIN 518210C / 518210C STLOC / 518210C RC</td>
<td>3</td>
</tr>
<tr>
<td>GSA HIGHLY ADAPTIVE CYBERSECURITY SERVICES LABOR CATEGORIES - SIN 54151HACS / 54151HACS STLOC / 54151HACS RC</td>
<td>13</td>
</tr>
<tr>
<td>GSA HEALTH IT SERVICES LABOR CATEGORIES - SIN 54151HEAL / 54151HEAL STLOC / 54151HEAL RC</td>
<td>28</td>
</tr>
<tr>
<td>GSA IT PROFESSIONAL SERVICES LABOR CATEGORIES - SIN 54151S / 54151S STLOC / 54151S RC</td>
<td>31</td>
</tr>
<tr>
<td>GSA IT SERVICES PRICELIST</td>
<td>42</td>
</tr>
<tr>
<td>USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS</td>
<td>45</td>
</tr>
<tr>
<td>BEST VALUE BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE</td>
<td>46</td>
</tr>
<tr>
<td>BASIC GUIDELINES FOR USING “CONTRACTOR TEAM ARRANGEMENTS”</td>
<td>48</td>
</tr>
</tbody>
</table>
CUSTOMER INFORMATION

1a. Table of Awarded Special Item Numbers (SINs):
   Please refer to GSA eLibrary (www.gsaelibrary.gsa.gov) for detailed SIN descriptions
   SIN 518210C / 518210C RC / 518210C STLOC, Cloud and Cloud-Related IT Professional Services
   SIN 54151HACS / 54151HACS RC / 54151HACS STLOC, Highly Adaptive Cybersecurity Solutions
   SIN 54151HEAL / 54151HEAL RC / 54151HEAL STLOC, Health Information Technology Services
   SIN 54151S / 54151S RC / 54151S STLOC, Professional Information Technology Services
   SIN OLM / OLM RC / OLM STLOC, Order Level Materials (OLM)

1b. Lowest Priced Model Number and Lowest Price:
   Please refer to our rates on page #42

1c. Labor Category Descriptions:
   Please refer to page #3

2. Maximum Order: $500,000.00
   Note: Agencies may place, and Contractor may honor, orders exceeding this limit in accordance with FAR 8.404

3. Minimum Order: $100.00

4. Geographic Coverage: Domestic delivery only

5. Point of Production: Not Applicable

6. Discount from List Price: All Prices Herein are Net

7. Quantity Discounts: None offered

8. Prompt Payment Terms: Net 30 days
   Information for Ordering Offices: Prompt payment terms cannot be negotiated out of the contractual agreement in exchange for other concessions.

9. Foreign Items: None

10a. Time of Delivery: As negotiated with Ordering Agency

10b. Expedited Delivery: Contact contractor for availability

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

10d. Urgent Requirement: Contact contractor for availability

11. F.O.B. Point: Destination

12a. Ordering Address: CollabraLink Technologies, Inc.
   8405 Greensboro Drive, Suite 600
   McLean, VA 22102
   Phone: (703) 639-1780
   Fax: (703) 639-1787

12b. For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPAs), are found in Federal Acquisition Regulation (FAR) 8.405-3.
13. Payment Address: CollabraLink Technologies, Inc.  
   Attn: Accounting  
   8405 Greensboro Drive, Suite 600  
   McLean, VA 22102  
   Phone: (703) 639-1780  
   Fax: (703) 639-1787

14. Warranty Provision: Not Applicable

15. Export Packing Charges: Not Applicable

16. Terms and conditions of rental, maintenance, and repair: Not Applicable

17. Terms and conditions of installation: Not Applicable

18a. Terms and conditions of repair parts indicating date of parts, price lists and any discounts from list prices: Not Applicable

18b. Terms and conditions for any other services: Not Applicable

19. List of service and distribution points: Not Applicable

20. List of participating dealers: Not Applicable

21. Preventative maintenance: Not Applicable

22a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants.): Not Applicable

22b. 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/  
   Contact Contractor for more information.

23. Unique Entity Identifier (UEI) Number: JNFEJMSLMXW7

24. CollabraLink Technologies, Inc. is registered in the System for Award Management (SAM).
Cloud Architect Level I
Minimum Experience/General Experience: Four years of experience.

Functional Responsibility: Designs and implements enterprise infrastructure and platforms required for cloud computing. Analyzes system requirements and ensures that systems will be securely integrated with current applications. Has a deep understanding of system development in cloud environments, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS). Reports to a manager or head of a unit/department. Work is generally independent and collaborative in nature.

Minimum Education:
- Bachelor's degree in area of specialty
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Architect Level II
Minimum Experience/General Experience: Seven years of experience.

Functional Responsibility: Designs and implements enterprise infrastructure and platforms required for cloud computing. Analyzes system requirements and ensures that systems will be securely integrated with current applications. Has a deep understanding of system development in cloud environments, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS). Reports to a manager or head of a unit/department. Work is generally independent and collaborative in nature.

Minimum Education:
- Bachelor's degree in area of specialty
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Architect Level III
Minimum Experience/General Experience: 10 years of experience.

Functional Responsibility: Designs and implements enterprise infrastructure and platforms required for cloud computing. Analyzes system requirements and ensures that systems will be securely integrated with current applications. Has a deep understanding of system development in cloud environments, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS). Reports to a manager or head of a unit/department. Work is generally independent and collaborative in nature.

Minimum Education:
- Bachelor’s degree in area of specialty
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Analyst Level I
Minimum Experience/General Experience: Two years of experience.

Functional Responsibility: Acquires/collects computer artifacts (e.g., malware, user activity, link files) in support of onsite engagements.
- Triage electronic devices and assess evidentiary value
- Correlates forensic findings to network events in support of developing an intrusion narrative
- Collects and documents system state information (e.g., running processes, network connections) prior to
imaging, as required
- Performs forensic triage of an incident to include determining scope, urgency and potential impact
- Tracks and documents forensic analysis from initial participation through resolution
- Collects, processes, preserves, analyzes and presents computer related evidence
- Coordinates with Government staff and customer personnel to validate/investigate alerts or additional preliminary findings
- Conducts analysis of forensic images, and available evidence in support of forensic write-ups for inclusion in reports and written products
- Documents and publishes Computer Network Defense (CND) guidance and reports pertaining to incident findings

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Analyst Level II

Minimum Experience/General Experience: Four years of experience.

Functional Responsibility: Acquires/collection computer artifacts (e.g., malware, user activity, link files) in support of onsite engagements
- Triage electronic devices and assess evidentiary value
- Correlates forensic findings to network events in support of developing an intrusion narrative
- Collects and documents system state information (e.g. running processes, network connections) prior to imaging, as required
- Performs forensic triage of an incident to include determining scope, urgency and potential impact
- Tracks and documents forensic analysis from initial participation through resolution
- Collects, processes, preserves, analyzes and presents computer related evidence
- Coordinates with Government staff and customer personnel to validate/investigate alerts or additional preliminary findings
- Conducts analysis of forensic images, and available evidence in support of forensic write-ups for inclusion in reports and written products
- Documents and publishes Computer Network Defense (CND) guidance and reports pertaining to incident findings

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Analyst Level III

Minimum Experience/General Experience: Six years of general experience in business analysis for information systems, including three years of process design

Functional Responsibility: Acquires/collection computer artifacts (e.g., malware, user activity, link files) in support of onsite engagements
- Triage electronic devices and assess evidentiary value
- Correlates forensic findings to network events in support of developing an intrusion narrative
- Collects and documents system state information (e.g. running processes, network connections) prior to imaging, as required
- Performs forensic triage of an incident to include determining scope, urgency and potential impact
- Tracks and documents forensic analysis from initial participation through resolution
- Collects, processes, preserves, analyzes and presents computer related evidence
- Coordinates with Government staff and customer personnel to validate/investigate alerts or additional preliminary findings
- Conducts analysis of forensic images, and available evidence in support of forensic write-ups for inclusion in reports and written products
- Documents and publishes Computer Network Defense (CND) guidance and reports pertaining to incident findings

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Operations Analyst Level I
Minimum Experience/General Experience: Two years of experience.

Functional Responsibility: Identifies, and mines relevant data from multiple sources. Cleans, reorganizes data, interprets data sets, find data trends and patterns valuable for diagnostics, predictive analytics efforts, and achieving business objectives
- Assists with the analysis, interpretation, and visualization of data. Collaborates with stakeholders to develop self-service business intelligence capabilities that enable business users to analyze cloud operational data and create data visualizations, BI dashboards and reports
- Manages cloud operations master data, including creation, updates, and deletion
- Manages and designs the reporting environment based on cloud operations data, including data sources, security, and metadata
- Provides quality assurance of cloud operations data, commission and decommission data sources and data sets
- Identifies, responds to, troubleshoots, and resolves data related operational and billing issues. Analyzes trends to proactively prevent incidents
- Manages the cloud operations data warehouse, identify, and support data needs for reporting requirements
- Supports initiatives for data integrity and normalization. Advocates for adoption of standardized data attributes and processes to improve cloud operations data integrity
- Provides technical expertise in cloud operations data storage architecture, data mining, and data cleansing. Participates in the design and maintenance of data systems and databases related to cloud operation, cloud billing, assist with strategic decisions on new systems
- Establishes strong working relationships, collaborate with clients, partners, Sales, Sales Operations, Corporate Operations, Cloud Operations, Finance, and IT Services to ensure data architecture design is scalable, data is accurate, timely, optimized, and able to support the business requirements of customers, partners, and internal users

Minimum Education:
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Operations Analyst Level II
Minimum Experience/General Experience: Six years of general experience in business analysis for information systems, including three years of process design.

Functional Responsibility: Identifies, and mines relevant data from multiple sources. Cleans, reorganizes data, interprets data sets, find data trends and patterns valuable for diagnostics, predictive analytics efforts, and achieving business objectives
- Assists with the analysis, interpretation, and visualization of data. Collaborates with stakeholders to
develop self-service business intelligence capabilities that enable business users to analyze cloud operational data and create data visualizations, BI dashboards and reports
- Manages cloud operations master data, including creation, updates, and deletion
- Manages and designs the reporting environment based on cloud operations data, including data sources, security, and metadata
- Provides quality assurance of cloud operations data, commission and decommission data sources and data sets
- Identifies, responds to, troubleshoots, and resolves data related operational and billing issues. Analyzes trends to proactively prevent incidents
- Manages the cloud operations data warehouse, identify, and support data needs for reporting requirements
- Supports initiatives for data integrity and normalization. Advocates for adoption of standardized data attributes and processes to improve cloud operations data integrity
- Provides technical expertise in cloud operations data storage architecture, data mining, and data cleansing. Participates in the design and maintenance of data systems and databases related to cloud operation, cloud billing, assist with strategic decisions on new systems
- Establishes strong working relationships, collaborate with clients, partners, Sales, Sales Operations, Corporate Operations, Cloud Operations, Finance, and IT Services to ensure data architecture design is scalable, data is accurate, timely, optimized, and able to support the business requirements of customers, partners, and internal users

Minimum Education:
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Operations Analyst Level III

Minimum Experience/General Experience: Seven years of IT experience with at least four years’ experience in a technical leadership.

Functional Responsibility: Identifies, and mines relevant data from multiple sources. Cleans, reorganizes data, interprets data sets, find data trends and patterns valuable for diagnostics, predictive analytics efforts, and achieving business objectives
- Assists with the analysis, interpretation, and visualization of data. Collaborates with stakeholders to develop self-service business intelligence capabilities that enable business users to analyze cloud operational data and create data visualizations, BI dashboards and reports
- Manages cloud operations master data, including creation, updates, and deletion
- Manages and designs the reporting environment based on cloud operations data, including data sources, security, and metadata
- Provides quality assurance of cloud operations data, commission and decommission data sources and data sets
- Identifies, responds to, troubleshoots, and resolves data related operational and billing issues. Analyzes trends to proactively prevent incidents
- Manages the cloud operations data warehouse, identify, and support data needs for reporting requirements
- Supports initiatives for data integrity and normalization. Advocates for adoption of standardized data attributes and processes to improve cloud operations data integrity
- Provides technical expertise in cloud operations data storage architecture, data mining, and data cleansing. Participates in the design and maintenance of data systems and databases related to cloud operation, cloud billing, assist with strategic decisions on new systems
- Establishes strong working relationships, collaborate with clients, partners, Sales, Sales Operations, Corporate Operations, Cloud Operations, Finance, and IT Services to ensure data architecture design is scalable, data is accurate, timely, optimized, and able to support the business requirements of customers, partners, and internal users
Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Site Reliability Engineer Level I
Minimum Experience/General Experience: Five years of general experience and three years of relevant Site Reliability Engineering experience.

Functional Responsibility: Focuses on uptime, performance, affordability, automation, scalability, and operational excellence. Strong knowledge of Linux and Cloud protocols along with a strong coding ability in Go, Python, and Bash.
- Administration experience with Linux including experience with the Linux kernel and Linux software packaging
- Strong software development skills in Go / Python / Bash.
- Strong skills in network services, including DNS, TLS/SSL and HTTP
- Network fundamentals DHCP, ARP, subnetting, routing, firewalls, IPv6
- Handle a project from the design phase to completion
- Experience dealing with bare metal hardware
- Experience dealing with cloud environments
- Performance analysis and debugging with various open-source tools
- Ansible and other configuration management systems
- Load balancing and reverse proxies such as Nginx, Varnish, HAProxy, Apache
- SQL databases (Postgres or MySQL)
- Time series databases (Clickhouse)
- Experience with even more databases such as MongoDB and Cassandra
- Internetworking and BGP Monitoring, DevOps, Design, Configuration Management, Container Orchestration

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Site Reliability Engineer Level II
Minimum Experience/General Experience: Seven years of general experience and three years of relevant Site Reliability Engineering experience.

Functional Responsibility: Focuses on uptime, performance, affordability, automation, scalability, and operational excellence. Strong knowledge of Linux and Cloud protocols along with a strong coding ability in Go, Python, and Bash.
- Administration experience with Linux including experience with the Linux kernel and Linux software packaging
- Strong software development skills in Go / Python / Bash.
- Strong skills in network services, including DNS, TLS/SSL and HTTP
- Network fundamentals DHCP, ARP, subnetting, routing, firewalls, IPv6
- Handle a project from the design phase to completion
- Experience dealing with bare metal hardware
- Experience dealing with cloud environments
- Performance analysis and debugging with various open-source tools
- Ansible and other configuration management systems
- Load balancing and reverse proxies such as Nginx, Varnish, HAProxy, Apache
- SQL databases (Postgres or MySQL)
- Time series databases (Clickhouse)
- Experience with even more databases such as MongoDB and Cassandra
- Internetworking and BGP Monitoring, DevOps, Design, Configuration Management, Container Orchestration

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Site Reliability Engineer Level III
Minimum Experience/General Experience: 10 years of general experience and three years of relevant Site Reliability Engineering experience.

Functional Responsibility: Focuses on uptime, performance, affordability, automation, scalability, and operational excellence. Strong knowledge of Linux and Cloud protocols along with a strong coding ability in Go, Python, and Bash.

- Administration experience with Linux including experience with the Linux kernel and Linux software packaging
- Strong software development skills in Go / Python / Bash.
- Strong skills in network services, including DNS, TLS/SSL and HTTP
- Network fundamentals DHCP, ARP, subnetting, routing, firewalls, IPv6
- Handle a project from the design phase to completion
- Experience dealing with bare metal hardware
- Experience dealing with cloud environments
- Performance analysis and debugging with various open-source tools
- Ansible and other configuration management systems
- Load balancing and reverse proxies such as Nginx, Varnish, HAProxy, Apache
- SQL databases (Postgres or MySQL)
- Time series databases (Clickhouse)
- Experience with even more databases such as MongoDB and Cassandra
- Internetworking and BGP Monitoring, DevOps, Design, Configuration Management, Container Orchestration

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Engineer Level II
Minimum Experience/General Experience: Seven years of experience.

Functional Responsibility: Implements and designs server, network, and software configurations for a cloud computing infrastructure and applications with a focus on DevOps principles. Monitors the performance of systems. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS).

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.
Cloud Engineer Level III  
**Minimum Experience/General Experience:** 10 years of experience.

**Functional Responsibility:** Implements and designs server, network, and software configurations for a cloud computing infrastructure and applications with a focus on DevOps principles. Monitors the performance of systems. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS).

**Minimum Education:**
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Migration Specialist Level I  
**Minimum Experience/General Experience:** Five years of experience.

**Functional Responsibility:** Develops migration strategies for applications, servers, etc. for a cloud computing infrastructure and applications with a focus on DevOps principles. Develops metrics, plans and acceptance criteria for the migration of systems. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS).

**Minimum Education:**
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Migration Specialist Level II  
**Minimum Experience/General Experience:** Seven years of experience.

**Functional Responsibility:** Develops migration strategies for applications, servers, etc. for a cloud computing infrastructure and applications with a focus on DevOps principles. Develops metrics, plans and acceptance criteria for the migration of systems. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS).

**Minimum Education:**
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Cloud Migration Specialist Level III  
**Minimum Experience/General Experience:** 10 years of experience.

**Functional Responsibility:** Develops migration strategies for applications, servers, etc. for a cloud computing infrastructure and applications with a focus on DevOps principles. Develops metrics, plans and acceptance criteria for the migration of systems. Familiar with standard concepts, practices, and procedures of cloud technology, including Software as Service (SaaS), Platform as Service (PaaS), or Infrastructure as a Service (IaaS).

**Minimum Education:**
- Bachelor's degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.
Azure/Google/AWS Cloud Security Engineer Level I

Minimum Experience/General Experience: Five years of IT experience; two years of experience with tools for vulnerability assessments and compliance reporting using eMASS, Xacta, ACAS, Continuous Monitoring and Risk Scoring (CMRS), Host-based Security System (HBSS), STIGs, or SRGs; two years of experience with cloud applications in a DevOps or DevSecOps environment; one year of experience with FedRamp

Functional Responsibility: Advise and assist with component organizations to comply with security guidance in their cloud application environments, including ensuring compliance with all Security Technical Implementation Guides (STIGs) and Ports and Protocols guidance. Analyze the design and building of, test, and Deploy technical solutions and processes to improve the efficiency and security of client cloud migrations and ensure compliance with necessary laws, regulations, and industry standards. Select and operate security and compliance tools, understand information security principles as they apply to Cloud-hosted applications, provide industry knowledge of DevSecOps trends and tools, and use technical expertise to implement technical solutions in either AWS, Google, or Azure cloud environments. Develops Risk Management artifacts, including SSP, SAP, SAR, RAR, and POA&M

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Azure/Google/AWS Cloud Security Engineer Level II

Minimum Experience/General Experience: Five years of IT experience; two years of experience with tools for vulnerability assessments and compliance reporting using eMASS, Xacta, ACAS, Continuous Monitoring and Risk Scoring (CMRS), Host-based Security System (HBSS), STIGs, or SRGs; two years of experience with cloud applications in a DevOps or DevSecOps environment; one year of experience with FedRamp

Functional Responsibility: Advise and assist with component organizations to comply with security guidance in their cloud application environments, including ensuring compliance with all Security Technical Implementation Guides (STIGs) and Ports and Protocols guidance. Analyze the design and building of, test, and Deploy technical solutions and processes to improve the efficiency and security of client cloud migrations and ensure compliance with necessary laws, regulations, and industry standards. Select and operate security and compliance tools, understand information security principles as they apply to Cloud-hosted applications, provide industry knowledge of DevSecOps trends and tools, and use technical expertise to implement technical solutions in either AWS, Google, or Azure cloud environments. Develops Risk Management artifacts, including SSP, SAP, SAR, RAR, and POA&M

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Azure/Google/AWS Cloud Security Engineer Level III

Minimum Experience/General Experience: Six years of IT experience; two years of experience with tools for vulnerability assessments and compliance reporting using eMASS, Xacta, ACAS, Continuous Monitoring and Risk Scoring (CMRS), Host-based Security System (HBSS), STIGs, or SRGs; two years of experience with cloud applications in a DevOps or DevSecOps environment; one year of experience with FedRamp

Functional Responsibility: Advise and assist with component organizations to comply with security guidance in their cloud application environments, including ensuring compliance with all Security Technical Implementation Guides (STIGs) and Ports and Protocols guidance. Analyze the design and building of, test, and Deploy technical solutions and processes to improve the efficiency and security of client cloud
migrations and ensure compliance with necessary laws, regulations, and industry standards. Select and operate security and compliance tools, understand information security principles as they apply to Cloud-hosted applications, provide industry knowledge of DevSecOps trends and tools, and use technical expertise to implement technical solutions in either AWS, Google, or Azure cloud environments. Develops Risk Management artifacts, including SSP, SAP, SAR, RAR, and POA&M

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

**IT Cloud Subject Matter Specialist Level I**

**Minimum Experience/General Experience:** One year of experience.

**Functional Responsibility:** Consults, plans, designs, and implements combined cloud and business process solutions. Develops and presents proof-of-concept for key decision makers. Analyzes business and software requirements. Provides exceptional technical pre-sales solutions. Oversees cloud solutions implementation and manage expectations.

**Minimum Education:**
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

**IT Cloud Subject Matter Specialist Level II**

**Minimum Experience/General Experience:** Four years of experience.

**Functional Responsibility:** Consults, plans, designs, and implements combined cloud and business process solutions. Develops and presents proof-of-concept for key decision makers. Analyzes business and software requirements. Provides exceptional technical pre-sales solutions. Oversees cloud solutions implementation and manage expectations.

**Minimum Education:**
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

**IT Cloud Subject Matter Specialist Level III**

**Minimum Experience/General Experience:** Seven years of experience.

**Functional Responsibility:** Consults, plans, designs, and implements combined cloud and business process solutions. Develops and presents proof-of-concept for key decision makers. Analyzes business and software requirements. Provides exceptional technical pre-sales solutions. Oversees cloud solutions implementation and manage expectations.

**Minimum Education:**
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

**Cloud Security Information Assurance Engineer Level II**

**Minimum Experience/General Experience:** Four years of experience.
Functional Responsibility: Determines enterprise information assurance and security standards. IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers’ requirements. Identifies, reports, and resolves security violations. Supports customers at the highest levels in the development and implementation of doctrine and policies. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Ensures that all information systems are functional and secure. Assist with identifying and review existing Enterprise Security Architecture (ESA) and developing new and continuous improving ESA Identifying and developing new Security Architecture Standards, Enterprise Architecture Security (EAS) Patterns, and Enterprise Security Processes and Procedures. Provide specialized cybersecurity knowledge and expertise to identify threats and manage risks from the adoption of new technologies including cloud, zero trust networking (ZTN); software defined networking (SDN), APIs, Data Analytics, and Dominance. Provide specialized knowledge and expertise with the NIST publications and requirements. Identify, evaluate, and recommend Enterprise Architecture Security (EAS) Standards to support Cybersecurity Framework functions Develop EAS in accordance with the Cybersecurity Policies and Best practices.

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

Cloud Security Information Assurance Engineer Level III

Minimum Experience/General Experience: Seven years of experience.

Functional Responsibility: Determines enterprise information assurance and security standards. IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. Develops and implements information assurance/security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Recommends information assurance/security solutions to support customers’ requirements. Identifies, reports, and resolves security violations. Supports customers at the highest levels in the development and implementation of doctrine and policies. Provides integration and implementation of the computer system security solution. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Ensures that all information systems are functional and secure. Assist with identifying and review existing Enterprise Security Architecture (ESA) and developing new and continuous improving ESA Identifying and developing new Security Architecture Standards, Enterprise Architecture Security (EAS) Patterns, and Enterprise Security Processes and Procedures. Provide specialized cybersecurity knowledge and expertise to identify threats and manage risks from the adoption of new technologies including cloud, zero trust networking (ZTN); software defined networking (SDN), APIs, Data Analytics, and Dominance. Provide specialized knowledge and expertise with the NIST publications and requirements. Identify, evaluate, and recommend Enterprise Architecture Security (EAS) Standards to support Cybersecurity Framework functions Develop EAS in accordance with the Cybersecurity Policies and Best practices.

Minimum Education:
- Bachelor’s degree
- An additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
Chief Cyber Information Security Officer

Minimum Experience/General Experience: Six years of managerial experience within one or more of the following disciplines: security operations, cyber risk and cyber intelligence, RMF, NIST, data loss and fraud prevention, security architecture, identity and access management, program management, Investigations and forensics or governance.

Functional Responsibility: Responsible for determining enterprise information security standards. Develop and implements cyber information security standards and procedures. Provide tactical information security advice and examining the ramifications of new technologies. Ensure that all information systems are functional and secure. In charge of IT risk evaluations, audits, and security incident investigation.

Minimum Education:
- Bachelors degree
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Chief Cyber Information Security Officer - Deputy

Minimum Experience/General Experience: Three years managerial experience in all phases of information security management. Experience directing employees and proficient in verbal and written communications skills. Ability to analyze, prioritize, organize, and solve problems.

Functional Responsibility: Assist the Chief Cyber Information Security Officer - Ensuring that all cyber information security management operations are functioning.

Minimum Education:
- Bachelors degree
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Cyber Security Specialist Level I

Minimum Experience/General Experience: Four years of experience

Functional Responsibility: Assists with the development and implementation of cyber information assurance (IA), and security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Performs analysis, design, and development of security features. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of systems and applications during all phases of the system development life cycle. Assists in the coordination and escalation of security incidents based on the tiered Incident Response approach. Has experience with experience in threat analysis, hunting, experience with multiple SIEMs and analyst detection workflow in the cloud. Performs at an entry-level or development level assignments. Build & deploy cloud security infrastructure and automate security operations for customers.

Minimum Education:
- Bachelors degree
- CompTIA Security+ ce OR GIAC Security Leadership (GSLC) OR Certified Authorization Professional (CAP) Certification
Cyber Security Specialist Level II

Minimum Experience/General Experience: Six years of experience.

Functional Responsibility: Assists with the development and implementation of cyber information assurance (IA), and security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Performs analysis, design, and development of security features. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of systems and applications during all phases of the system development life cycle. Assists in the coordination and escalation of security incidents based on the tiered Incident Response approach. Has experience with threat analysis, hunting, experience with multiple SIEMs and analyst detection workflow in the cloud. Performs at an entry-level or development level assignments. Build & deploy cloud security infrastructure and automate security operations for customers.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR CompTIA Advanced Security Practitioner+ (CASP+ ce) OR Certified Authorization Professional (CAP) Certification

Cyber Security Specialist Level III

Minimum Experience/General Experience: Nine years of experience

Functional Responsibility: Assists with the development and implementation of cyber information assurance (IA), and security standards and procedures. Coordinates, develops, and evaluates security programs for an organization. Performs analysis, design, and development of security features. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Performs vulnerability/risk analyses of systems and applications during all phases of the system development life cycle. Assists in the coordination and escalation of security incidents based on the tiered Incident Response approach. Has experience with threat analysis, hunting, experience with multiple SIEMs and analyst detection workflow in the cloud. Performs at an entry-level or development level assignments. Build & deploy cloud security infrastructure and automate security operations for customers.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR GIAC Security Leadership (GSLC) OR Certified Chief Information Security Officer (CCISO) Certification

Cyber Data Scientist / Cyber Data Analyst

Minimum Experience/General Experience: Six years of experience

Functional Responsibility: Adept at combining techniques from machine learning and statistics to solve cyber security tasks. Leverages machine learning algorithms as substantiation parts in any well-known security products such as Intrusion detection and prevention systems, Security orchestration, Behavioral authentications, Endpoint detection, Data leakage prevention, Vulnerability prioritization. Set up Machine learning algorithms in support of Security standards and procedures. Has experience with Data Science, Analytics and Cyber security with applicable certifications.

Minimum Education:
- Bachelors degree in Computer Science, Information Systems, Business, Management, or Equivalent.
- Appian Certifications: Active A-score level of 2 or one year hands-on Appian solution implementation experience.
- Certification(s) on Agile methodology
Cyber Information Security Analyst Level I
Minimum Experience/General Experience: Four years of experience with Federal Information Security Management Act (FISMA) compliance.

Functional Responsibility: Analyze and define cyber security requirements. Assists in the design, development, and implementation of solutions. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Assists in the performance of risk analyses which includes risk assessment.

Minimum Education:
- Bachelors degree
- CompTIA Security+ ce OR GIAC Security Leadership (GSLC) OR Certified Authorization Professional (CAP) Certification

Cyber Information Security Analyst Level II
Minimum Experience/General Experience: Six years of experience with Federal Information Security Management Act (FISMA) compliance.

Functional Responsibility: Analyze and define cyber security requirements. Assists in the design, development, and implementation of solutions. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Assists in the performance of risk analyses which includes risk assessment.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR CompTIA Advanced Security Practitioner+ (CASP+ ce) OR Certified Authorization Professional (CAP) Certification

Cyber Information Security Analyst Level III

Functional Responsibility: Analyze and define cyber security requirements. Assists in the design, development, and implementation of solutions. Gathers and organizes technical information about an organization's mission goals and needs, existing security products, and ongoing programs. Assists in the performance of risk analyses which includes risk assessment.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR GIAC Security Leadership (GSLC) OR Certified Chief Information Security Officer (CCISO) Certification

Cyber Security Information Assurance Engineer Level I
Minimum Experience/General Experience: Three years of experience.

Functional Responsibility: Determines enterprise information assurance and security standards. IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
• Provides integration and implementation of the computer system security solution.
• Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
• Ensures that all information systems are functional and secure.
• assist with identifying and review existing Enterprise Security Architecture (ESA) and developing new and continuous improving ESA
• Provide specialized cybersecurity knowledge and expertise to identify threats and manage risks from the adoption of new technologies including cloud, zero trust networking (ZTN); software defined networking (SDN), APIs, Data Analytics, and Dominance.
• Provide specialized knowledge and expertise with the NIST publications and requirements.
• Identify, evaluate, and recommend Enterprise Architecture Security (EAS) Standards to support Cybersecurity Framework functions
• Develop EAS in accordance with the Cybersecurity Policies and Best practices.

Minimum Education:
• Bachelors degree

Cyber Security Information Assurance Engineer Level II
Minimum Experience/General Experience: Six years of experience on a technical development team in the areas of software and application development. Familiarity with standard concepts, practices, and procedures within the area of technical development. Knowledge of full cycle software development and relational database concepts.

Functional Responsibility: Determines enterprise information assurance and security standards. IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
• Develops and implements information assurance/security standards and procedures.
• Coordinates, develops, and evaluates security programs for an organization.
• Recommends information assurance/security solutions to support customers' requirements.
• Identifies, reports, and resolves security violations.
• Supports customers at the highest levels in the development and implementation of doctrine and policies.
• Provides integration and implementation of the computer system security solution.
• Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
• Ensures that all information systems are functional and secure.
• assist with identifying and review existing Enterprise Security Architecture (ESA) and developing new and continuous improving ESA
• Provide specialized cybersecurity knowledge and expertise to identify threats and manage risks from the adoption of new technologies including cloud, zero trust networking (ZTN); software defined networking (SDN), APIs, Data Analytics, and Dominance.
• Provide specialized knowledge and expertise with the NIST publications and requirements.
• Identify, evaluate, and recommend Enterprise Architecture Security (EAS) Standards to support Cybersecurity Framework functions
• Develop EAS in accordance with the Cybersecurity Policies and Best practices.

Minimum Education:
• Bachelors degree
Cyber Security Information Assurance Engineer Level III

Minimum Experience/General Experience: Nine years of experience.

Functional Responsibility: Determines enterprise information assurance and security standards. IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Provides integration and implementation of the computer system security solution.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Ensures that all information systems are functional and secure.
- Assist with identifying and review existing Enterprise Security Architecture (ESA) and developing new and continuous improving ESA
- Provide specialized cybersecurity knowledge and expertise to identify threats and manage risks from the adoption of new technologies including cloud, zero trust networking (ZTN); software defined networking (SDN), APIs, Data Analytics, and Dominance.
- Provide specialized knowledge and expertise with the NIST publications and requirements.
- Identify, evaluate, and recommend Enterprise Architecture Security (EAS) Standards to support Cybersecurity Framework functions
- Develop EAS in accordance with the Cybersecurity Policies and Best practices.

Minimum Education:

- Bachelors degree

Windows Cyber System Security Engineer Level I

Minimum Experience/General Experience: Four years of experience.

Functional Responsibility:

- Designs and implements cyber network topologies
- Maintains and troubleshoots operational networks including VPN, routers, switches, firewalls, and similar network equipment.
- Applies patching to network infrastructure equipment
- Contributes to development of network architecture documentation
- Participates in network security assessments, remediation, and documentation, Strong understanding of network infrastructure and associated, network hardware and software.
- Experience defining and configuring complex networks governed by comprehensive security guidelines
- Ability to apply analytical and problem-solving skills to resolve network issues
- Ability to implement, administer, and troubleshoot network infrastructure devices, such as: firewalls, routers, switches, backup appliances
- Creating, updating, and managing network security documentation and diagrams.
- Provides specific detailed information for hardware and software selection.

Minimum Education:

- Bachelors degree
- CompTIA Security+ ce OR GIAC Security Leadership (GSLC) OR Certified Authorization Professional (CAP) Certification
Windows Cyber System Security Engineer Level II
Minimum Experience/General Experience: Six years of experience.

Functional Responsibility:
- Designs and implements cyber network topologies
- Maintains and troubleshoots operational networks including VPN, routers, switches, firewalls, and similar network equipment.
- Applies patching to network infrastructure equipment
- Contributes to development of network architecture documentation
- Participates in network security assessments, remediation, and documentation, Strong understanding of network infrastructure and associated, network hardware and software.
- Experience defining and configuring complex networks governed by comprehensive security guidelines
- Ability to apply analytical and problem-solving skills to resolve network issues
- Ability to implement, administer, and troubleshoot network infrastructure devices, such as: firewalls, routers, switches, backup appliances.
- Creating, updating, and managing network security documentation and diagrams.
- Provides specific detailed information for hardware and software selection.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR CompTIA Advanced Security Practitioner+ (CASP+ ce) OR Certified Authorization Professional (CAP) Certification

Windows Cyber System Security Engineer Level III
Minimum Experience/General Experience: Nine years of experience.

Functional Responsibility:
- Designs and implements cyber network topologies
- Maintains and troubleshoots operational networks including VPN, routers, switches, firewalls, and similar network equipment.
- Applies patching to network infrastructure equipment
- Contributes to development of network architecture documentation
- Participates in network security assessments, remediation, and documentation, Strong understanding of network infrastructure and associated, network hardware and software.
- Experience defining and configuring complex networks governed by comprehensive security guidelines
- Ability to apply analytical and problem-solving skills to resolve network issues
- Ability to implement, administer, and troubleshoot network infrastructure devices, such as: firewalls, routers, switches, backup appliances.
- Creating, updating, and managing network security documentation and diagrams.
- Provides specific detailed information for hardware and software selection.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR GIAC Security Leadership (GSLC) OR Certified Chief Information Security Officer (CCISO) Certification

Cyber Penetration Tester Level I
Minimum Experience/General Experience: Four years of experience.

Functional Responsibility: Performs security tests on cyber networks, web-based applications, and computer systems. Designs these tests and tools to try to break into security-protected applications and networks to
probe for vulnerabilities. Evaluates new penetration testing tools. Exploits vulnerabilities and design solutions to security issues like temperature, humidity, vandalism, and natural disasters. Conducts network and system security audits, which evaluate how well an organization’s system conforms to a set of established criteria. Analyzes Security policies for effectiveness, makes suggestions on security policy improvements, and works to enhance methodology material. Provides feedback and verification after security fixes are issued.

Minimum Education:
- Bachelors degree
- CompTIA Security+ (GSLC) OR Certified Authorization Professional (CAP) Certification

Cyber Penetration Tester Level II
Minimum Experience/General Experience: Six years of experience.

Functional Responsibility: Performs security tests on cyber networks, web-based applications, and computer systems. Designs these tests and tools to try to break into security-protected applications and networks to probe for vulnerabilities. Evaluates new penetration testing tools. Exploits vulnerabilities and design solutions to security issues like temperature, humidity, vandalism, and natural disasters. Conducts network and system security audits, which evaluate how well an organization’s system conforms to a set of established criteria. Analyzes Security policies for effectiveness, makes suggestions on security policy improvements, and works to enhance methodology material. Provides feedback and verification after security fixes are issued.

Minimum Education:
- Bachelors degree

Cyber Penetration Tester Level III
Minimum Experience/General Experience: Nine years of experience.

Functional Responsibility: Performs security tests on cyber networks, web-based applications, and computer systems. Designs these tests and tools to try to break into security-protected applications and networks to probe for vulnerabilities. Evaluates new penetration testing tools. Exploits vulnerabilities and design solutions to security issues like temperature, humidity, vandalism, and natural disasters. Conducts network and system security audits, which evaluate how well an organization’s system conforms to a set of established criteria. Analyzes Security policies for effectiveness, makes suggestions on security policy improvements, and works to enhance methodology material. Provides feedback and verification after security fixes are issued.

Minimum Education:
- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR GIAC Security Leadership (GSLC) OR Certified Chief Information Security Officer (CCISO) Certification

Cyber Threat Intelligence Analyst Level I
Minimum Experience/General Experience: Four years of experience.

Functional Responsibility:
- Provides knowledge in threat intelligence and cyber security defense.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Identifies, deters, monitors, and investigates computer and network intrusions.
- Provides computer forensic support to high technology investigations in the form of evidence seizure,
computer forensic analysis, and data recovery.

- Conducts incident response according to departmental breach response process.
- Leads threat intelligence and incident response.
- Coordinates with high authorities as necessary.
- Ensures an optimal security posture by identifying ongoing, immediate, and emerging threats to the organization, including insider threats, threat actors, attack vectors, and breach scenarios.
- Provides support utilizing underlying tools to profile and assess insider threat and potential fraud.
- Develops, maintains, and optimizes an automated integration system to receive, leverage, and disseminate cyber threat intelligence identified from multiple classified and open sources for detecting, tracking, preventing, and responding to threats and threat actors.
- Creates Incident Response Threat Package - per incident.
- Monitors threat intelligence sources (security alerts, warnings, and other indicators) from the U.S. Computer Emergency Readiness Team (US-CERT), and other OSINT sources to compile client-related threat intelligence.
- Provides cyber-threat intelligence on client-related topics including.
- Provides cyber-threat intelligence on cyber campaigns against U.S. information technology that could potentially affect the client’s portfolio for systems and the Institutions of Higher Education that the client is responsible for supporting.
- Provides cyber-threat intelligence on a cyber-related attack against the federal/private education sector.
- Conducts threat operations to identify Department or education data that may be available through unauthorized sources (Dark Net, hacking sites, etc.).
- Provides any intelligence on information technology vulnerabilities being reported across the federal and private sectors.

Minimum Education:
- Bachelors degree

Cyber Threat Intelligence Analyst Level II

Minimum Experience/General Experience: Six years of experience.

Functional Responsibility:

- Provides knowledge in threat intelligence and cyber security defense.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Identifies, deters, monitors, and investigates computer and network intrusions.
- Provides computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery.
- Conducts incident response according to departmental breach response process.
- Leads threat intelligence and incident response.
- Coordinates with high authorities as necessary.
- Ensures an optimal security posture by identifying ongoing, immediate, and emerging threats to the organization, including insider threats, threat actors, attack vectors, and breach scenarios.
- Provides support utilizing underlying tools to profile and assess insider threat and potential fraud.
- Develops, maintains, and optimizes an automated integration system to receive, leverage, and disseminate cyber threat intelligence identified from multiple classified and open sources for detecting, tracking, preventing, and responding to threats and threat actors.
- Creates Incident Response Threat Package - per incident.
- Monitors threat intelligence sources (security alerts, warnings, and other indicators) from the U.S. Computer Emergency Readiness Team (US-CERT), and other OSINT sources to compile client-related threat intelligence.
- Provides cyber-threat intelligence on client-related topics including.
- Provides cyber-threat intelligence on cyber campaigns against U.S. information technology that could potentially affect the client’s portfolio for systems and the Institutions of Higher Education that the client
is responsible for supporting.

- Provides cyber-threat intelligence on a cyber-related attack against the federal/private education sector.
- Conducts threat operations to identify Department or education data that may be available through unauthorized sources (Dark Net, hacking sites, etc.).
- Provides any intelligence on information technology vulnerabilities being reported across the federal and private sectors.

Minimum Education:

- Bachelors degree

**Cyber Threat Intelligence Analyst Level III**

Minimum Experience/General Experience: Nine years experience.

**Functional Responsibility:**

- Provides knowledge in threat intelligence and cyber security defense.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Identifies, deters, monitors, and investigates computer and network intrusions.
- Provides computer forensic support to high technology investigations in the form of evidence seizure, computer forensic analysis, and data recovery.
- Conducts incident response according to departmental breach response process.
- Leads threat intelligence and incident response.
- Coordinates with high authorities as necessary.
- Ensures an optimal security posture by identifying ongoing, immediate, and emerging threats to the organization, including insider threats, threat actors, attack vectors, and breach scenarios.
- Provides support utilizing underlying tools to profile and assess insider threat and potential fraud.
- Develops, maintains, and optimizes an automated integration system to receive, leverage, and disseminate cyber threat intelligence identified from multiple classified and open sources for detecting, tracking, preventing, and responding to threats and threat actors.
- Creates Incident Response Threat Package - per incident.
- Monitors threat intelligence sources (security alerts, warnings, and other indicators) from the U.S. Computer Emergency Readiness Team (US-CERT), and other OSINT sources to compile client-related threat intelligence.
- Provides cyber-threat intelligence on client-related topics including.
- Provides cyber-threat intelligence on cyber campaigns against U.S. information technology that could potentially affect the client’s portfolio for systems and the Institutions of Higher Education that the client is responsible for supporting.
- Provides cyber-threat intelligence on a cyber-related attack against the federal/private education sector.
- Conducts threat operations to identify Department or education data that may be available through unauthorized sources (Dark Net, hacking sites, etc.).
- Provides any intelligence on information technology vulnerabilities being reported across the federal and private sectors.

Minimum Education:

- Bachelors degree

**Cyber Security Tools Engineer/Cyber Engineering Subject Matter Specialist Level II**

Minimum Experience/General Experience: Three years of experience.

**Functional Responsibility:**

- Designs and architects tools to maximize the effectiveness of tools individually or as part of a defensive grid
- Provides support to staff who are installing and configuring Security tools, while learning both skill sets.
- Designs scripts, dashboards, etc. to monitor the tools to insure proper operations and performance
- Engineers Security tools to report to network monitoring tools via Syslog/SNMP
- Assist staff in troubleshooting tool issues
- Integrates and tests new code versions and upgrades in the Security lab prior to deployment to production

**Minimum Education:**
- Bachelors degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

**Cyber Security Tools Engineer/Cyber Engineering Subject Matter Specialist Level III**

**Minimum Experience/General Experience:** Nine years of experience.

**Functional Responsibility:**
- Designs and architects tools to maximize the effectiveness of tools individually or as part of a defensive grid
- Provides support to staff who are installing and configuring Security tools, while learning both skill sets.
- Designs scripts, dashboards, etc. to monitor the tools to insure proper operations and performance
- Engineers Security tools to report to network monitoring tools via Syslog/SNMP
- Assist staff in troubleshooting tool issues
- Integrates and tests new code versions and upgrades in the Security lab prior to deployment to production

**Minimum Education:**
- Bachelors degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

**Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level I**

**Minimum Experience/General Experience:** Four years of experience.

**Functional Responsibility:** Verifies that the code is a correct and effective solution for cyber security and vulnerability requirements. Ensures that code is maintainable and follows best practices. Increases security knowledge of the codebase and provides patching and best practices as applicable. Supports security operations, assessments, and POA&M development.

**Minimum Education:**
- Bachelors degree

**Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level II**

**Minimum Experience/General Experience:** Six years of experience.

**Functional Responsibility:** Verifies that the code is a correct and effective solution for cyber security and vulnerability requirements. Ensures that code is maintainable and follows best practices. Increases security knowledge of the codebase and provides patching and best practices as applicable. Supports security operations, assessments, and POA&M development.

**Minimum Education:**
- Bachelors degree
Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level III

Minimum Experience/General Experience: Nine years of experience.

Functional Responsibility: Verifies that the code is a correct and effective solution for cyber security and vulnerability requirements. Ensures that code is maintainable and follows best practices. Increases security knowledge of the codebase and provides patching and best practices as applicable. Supports security operations, assessments, and POA&M development.

Minimum Education:
- Bachelors degree

Cyber Vulnerability Analyst Level I

Minimum Experience/General Experience: Four years of experience.

Functional Responsibility:
- Provides knowledge in cyber vulnerability management and POA&M support.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Supports customers at the highest levels in the development and implementation of doctrine and policies. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Supports security operations, assessments, and POA&M development.

Minimum Education:
- Bachelors degree

Cyber Vulnerability Analyst Level II

Minimum Experience/General Experience: Six years of experience.

Functional Responsibility:
- Provides knowledge in cyber vulnerability management and POA&M support.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Supports customers at the highest levels in the development and implementation of doctrine and policies. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Supports security operations, assessments, and POA&M development.

Minimum Education:
- Bachelors degree
Cyber Vulnerability Analyst Level III
Minimum Experience/General Experience: Nine years of experience.

Functional Responsibility:
- Provides knowledge in cyber vulnerability management and POA&M support.
- Develops, researches, and maintains proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.
- Determines enterprise information assurance and security standards.
- Develops and implements information assurance/security standards and procedures.
- Coordinates, develops, and evaluates security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Supports customers at the highest levels in the development and implementation of doctrine and policies. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Supports security operations, assessments, and POA&M development.

Minimum Education:
- Bachelors degree

Cyber SOC Analyst Level I
Minimum Experience/General Experience: Four years of experience.

Functional Responsibility:
- Coordinates, develops, and evaluates cyber security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the systems development life cycle.
- Provides Proactive/reactive incident handling, security event management, forensics, vulnerability management, audit/penetration testing, advising of proper security measures, encouraging industry best security practices, managing telephone trouble calls, issuance of Information System Security (ISS) Alerts.
- Performs the initial triage and provides remediation instructions to the appropriate response teams.
- Provide periodic vulnerability scanning of critical devices and recommends steps to mitigate risk and exposure to attacks.
- Provides SOC operations support at the Tier 1 & Tier 2 level providing 24x7x365 day a year immediate cybersecurity response activities.
- Supports the operations of security capabilities to provide continuous monitoring of assigned assets, networks, and data locations.

Tier 1 - Triage:
- Reviewing and assigning urgency to potential threats.
- Function as the front line when reporting security incidents.
Run vulnerability and security assessment reports, manage security-monitoring tools, and perform cybersecurity incident helpdesk functions.

Tier 2 - Incident Response:
- Leverages security controls, policies, and intelligence (indicators of compromise (IOC), rules, and procedures) to determine the scope and origin of the attack.
- Focus on mitigation, recovery, and remediation once an attack has occurred.
- Communicates threat information and other relevant security data and alerts to information system stakeholders

Minimum Education:
- Bachelors degree

Cyber SOC Analyst Level II
Minimum Experience/General Experience: Six years of experience.

Functional Responsibility:
- Coordinates, develops, and evaluates cyber security programs for an organization.
- Recommends information assurance/security solutions to support customers’ requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the systems development life cycle.
- Provides Proactive/reactive incident handling, security event management, forensics, vulnerability management, audit/penetration testing, advising the of proper security measures, encouraging industry best security practices, managing telephone trouble calls, issuance of Information System Security (ISS) Alerts.
- Performs the initial triage and provides remediation instructions to the appropriate response teams.
- Provide periodic vulnerability scanning of critical devices and recommends steps to mitigate risk and exposure to attacks.
- Provides SOC operations support at the Tier 1 & Tier 2 level providing 24x7x365 day a year immediate cybersecurity response activities.
- Supports the operations of security capabilities to provide continuous monitoring of assigned assets, networks, and data locations.

Tier 1 - Triage:
- Reviewing and assigning urgency to potential threats.
- Function as the front line when reporting security incidents.
- Run vulnerability and security assessment reports, manage security-monitoring tools, and perform cybersecurity incident helpdesk functions.

Tier 2 - Incident Response:
- Leverages security controls, policies, and intelligence (indicators of compromise (IOC), rules, and procedures) to determine the scope and origin of the attack.
- Focus on mitigation, recovery, and remediation once an attack has occurred.
- Communicates threat information and other relevant security data and alerts to information system stakeholders
Minimum Education:

- Bachelors degree

**Cyber SOC Analyst Level III**

Minimum Experience/General Experience: Nine year of experience.

**Functional Responsibility:**

- Coordinates, develops, and evaluates cyber security programs for an organization.
- Recommends information assurance/security solutions to support customers' requirements.
- Identifies, reports, and resolves security violations.
- Establishes and satisfies information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands.
- Supports customers at the highest levels in the development and implementation of doctrine and policies.
- Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems.
- Performs vulnerability/risk analyses of computer systems and applications during all phases of the systems development life cycle.
- Provides Proactive/reactive incident handling, security event management, forensics, vulnerability management, audit/penetration testing, advising the of proper security measures, encouraging industry best security practices, managing telephone trouble calls, issuance of Information System Security (ISS) Alerts.
- Performs the initial triage and provides remediation instructions to the appropriate response teams.
- Provide periodic vulnerability scanning of critical devices and recommends steps to mitigate risk and exposure to attacks.
- Provides SOC operations support at the Tier 1 & Tier 2 level providing 24x7x365 day a year immediate cybersecurity response activities.
- Supports the operations of security capabilities to provide continuous monitoring of assigned assets, networks, and data locations.

**Tier 1 - Triage:**

- Reviewing and assigning urgency to potential threats.
- Function as the front line when reporting security incidents.
- Run vulnerability and security assessment reports, manage security-monitoring tools, and perform cybersecurity incident helpdesk functions.

**Tier 2 - Incident Response:**

- Leverages security controls, policies, and intelligence (indicators of compromise (IOC), rules, and procedures) to determine the scope and origin of the attack.
- Focus on mitigation, recovery, and remediation once an attack has occurred.
- Communicates threat information and other relevant security data and alerts to information system stakeholders

Minimum Education:

- Bachelors degree

**Cyber SIEM Engineer Level I**

Minimum Experience/General Experience: Four years of experience with AWS or similar certificate(s). Four years of experience in security related areas such as vulnerability management, penetration testing, SIEM, Data, Protect, Secure, Cloud. Experience with a Configuration Management tool (Ansible, Saltstack, Puppet, Chef); Ansible or SaltStack preferred.

**Functional Responsibility:** Administers data feeds to ensure accurate normalization through parsing and
scripting. Reports, with dashboarding, alerting and other analytical tasks in Splunk. Protects the network and secures the cyber mission. Administration, deployment, and use of Splunk and other SIEM. Experienced with Linux administration. Performs log normalization and other scripting and parsing (including a variety of formats such as CEF, JSON, XML, etc…).

Minimum Education:

- Bachelors degree
- CompTIA Security+ OR GIAC Security Leadership (GSLC) OR Certified Authorization Professional (CAP) Certification

**Cyber SIEM Engineer Level II**

Minimum Experience/General Experience: Six years of experience with AWS or similar certificate(s). Six years of experience in security related areas such as vulnerability management, penetration testing, SIEM, Data, Protect, Secure, Cloud. Experience with a Configuration Management tool (Ansible, Saltstack, Puppet, Chef); Ansible or SaltStack preferred.

Functional Responsibility: Administers data feeds to ensure accurate normalization through parsing and scripting. Reports, with dashboarding, alerting and other analytical tasks in Splunk. Protects the network and secures the cyber mission. Administration, deployment, and use of Splunk and other SIEM. Experienced with Linux administration. Performs log normalization and other scripting and parsing (including a variety of formats such as CEF, JSON, XML, etc…).

Minimum Education:

- Bachelors degree
- Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) OR CompTIA Advanced Security Practitioner+ (CASP+ ce) OR Certified Authorization Professional (CAP) Certification
Health IT Application Engineer I

Minimum Experience/General Experience: Four years of experience provisioning, configuring, deploying, and supporting Health IT applications or other software applications, as well as their supporting tools and services, in a healthcare and/or clinical environment.

Functional Responsibility: Under general supervision, identify specific healthcare and/or clinical customer needs, develop Health IT solutions to those needs, and provide guidance on how to integrate those solutions into the overall service delivery model.

Minimum Education:
- Bachelor's degree in Computer Science or a related technical discipline
- An additional four years of equivalent work experience and an Associate's degree or an additional eight years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor's degree.

Health IT Business Analyst

Minimum Experience/General Experience: Four years of experience in a related field. May have expert credentials or be recognized as an authority.

Functional Responsibility: Formulates and defines Health IT systems scope and objectives through research and fact-finding combined with an understanding of applicable healthcare systems and industry requirements. Performs analysis of clinical and user needs, documenting requirements, and revising existing system logic difficulties as necessary. Competent to work in all phases of Health IT systems analysis and considers the healthcare implications of the application of technology to the specific clinical environment.

Minimum Education:
- Bachelors degree in Business, Finance, Management, Information Systems or another applicable field.
- An additional four years of experience and an Associate's degree or an additional eight years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Health IT IM/IT I

Minimum Experience/General Experience: Two years of Health IT engineering experience. Must possess system engineering experience in one or more areas including telecommunications concepts, computer languages, operating systems, database/DBMS and middleware.

Functional Responsibility: Under direct supervision analyzes functional business requirements and design specifications for Health IT solutions. Identifies and resolves problems within existing Health IT systems and designs/implements new systems, enhances the existing systems, and participates in analysis, design, and new construction of next generation Health IT systems. Responsible for understanding the needs of the customers and the capabilities of commercially available Heath IT products and general IT products used in healthcare and/or clinical environments. Assists in creation of requirements for implementation by the architecture and engineering teams using COTS products.

Minimum Education:
- Bachelor's degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.
Health IT IM/IT II

Minimum Experience/General Experience: Four years of Health IT engineering experience. Must possess system engineering experience in one or more areas including telecommunications concepts, computer languages, operating systems, database/DBMS and middleware.

Functional Responsibility: Under general supervision analyzes functional business requirements and design specifications for Health IT solutions. Identifies and resolves problems within existing Health IT systems and designs/implements new systems, enhances the existing systems, and participates in analysis, design, and new construction of next generation Health IT systems. Responsible for understanding the needs of the customers and the capabilities of commercially available Health IT products and general IT products used in healthcare and/or clinical environments. Creates requirements for implementation by the architecture and engineering teams using COTS products.

Minimum Education:
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Health IT Project Manager

Minimum Experience/General Experience: Six years of experience required specializing in Health IT focused projects. Experience in project management plan development including project scheduling, resource allocation, and budgeting. Experience across all PMBOK project management lifecycle phases including initiating; planning; executing; monitoring and controlling; and closing. Experience in managing IT projects in healthcare and/or clinical settings.

Functional Responsibility: Manage projects, tasks, and/or subtasks. Advise and assist project staff on execution of specific project requirements. May be responsible for management of complete project or specific task elements. Implements directives and schedules necessary to ensure effective project management. Possesses a detailed knowledge of concepts, practices, and procedures in several activity, technical, and management fields. Provides oversight of complex projects in healthcare and/or clinical settings and provides detailed guidance and direction to project staff.

Minimum Education:
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Health IT Software Consultant I

Minimum Experience/General Experience: Two years of experience in implementing Health IT software applications or hands-on experience with healthcare software applications. Familiarity with relational database concepts and client-server architectures.

Functional Responsibility: Under direct supervision, reviews, analyzes, and modifies Health IT software systems or software systems employed in a healthcare/clinical environment including encoding, testing, debugging, and installing to support an organization’s applications systems. May be expected to write documentation to describe program development, logic, coding, and corrections. Writes manual for users to describe installation and operating procedures.

Minimum Education:
- Bachelors degree.
- An additional two years of equivalent work experience and an Associate’s degree or an additional four years of equivalent work experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
Health IT Software Consultant II

Minimum Experience/General Experience: Five years of experience in implementing Health IT software applications or hands-on experience with healthcare software applications. Familiarity with relational database concepts and client-server architectures. Relies on experience and judgment to plan and accomplish goals.

Functional Responsibility: Reviews, analyzes, and modifies Health IT software systems or software systems employed in a healthcare/clinical environment including encoding, testing, debugging, and installing to support an organization’s applications systems. Consults with users to identify current operating procedures and to clarify program objectives. May be expected to write documentation to describe program development, logic, coding, and corrections. Writes manual for users to describe installation and operating procedures.

Minimum Education:

- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.
Financial Analyst
Minimum Experience/General Experience: Four years of experience in a related field

Functional Responsibility: Participates in the development of budgets. Determines cost of operations by establishing standard costs and collecting operational data. Develops forecasts and determines financial status by comparing and analyzing actual results with plans and forecasts. Establishes and enforces financial policies and procedure. Improves financial status by analyzing results, monitoring variances, identifying trends, and recommending actions to management. Reconciles transactions by comparing and correcting data.

Minimum Education:
- Bachelors degree in Business, Finance, Management, Information Systems or another applicable field.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Technical Business Analyst I
Minimum Experience/General Experience: Two years of experience in a related field.

Functional Responsibility: Under direct supervision, formulates and defines systems scope and objectives through research and fact-finding combined with an understanding of applicable business systems and industry requirements. Performs analysis of business and user needs, documenting requirements, and revising existing system logic difficulties as necessary.

Minimum Education:
- Bachelors degree in Business, Finance, Management, Information Systems or another applicable field.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience

Technical Business Analyst II
Minimum Experience/General Experience: Four years of experience in a related field.

Functional Responsibility: Under general supervision, formulates and defines systems scope and objectives through research and fact-finding combined with an understanding of applicable business systems and industry requirements. Performs analysis of business and user needs, documenting requirements, and revising existing system logic difficulties as necessary. Guides and advises less-experienced Business Analysts. Competent to work in some phases of systems analysis and considers the business implications of the application of technology to the current business environment.

Minimum Education:
- Bachelors degree in Business, Finance, Management, Information Systems or another applicable field.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.
Technical Business Analyst III

Minimum Experience/General Experience: Six years of experience in a related field. May have expert credentials or be recognized as an authority.

Functional Responsibility: Formulates and defines systems scope and objectives through research and fact-finding combined with an understanding of applicable business systems and industry requirements. Performs analysis of business and user needs, documenting requirements, and revising existing system logic difficulties as necessary. Guides and advises less experienced Business Analysts. Competent to work in all phases of systems analysis and considers the business implications of the application of technology to the current business environment.

Minimum Education:
- Bachelors degree in Business, Finance, Management, Information Systems or another applicable field.
- An additional four (4) years of experience and an Associate's degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Change, Configuration, and Release Manager

Minimum Experience/General Experience: Four years of experience in a related field.

Functional Responsibility: Responsible for change, configuration, and release management planning. Describes provisions for configuration identification, change control, configuration status accounting, and configuration audits. Responsible for configuration planning. Identifies and maintains the original configuration of requirements documentation, design documentation, and related documentation. Responsible for configuration change control.

Regulates the change process so that only approved and validated changes are incorporated into product documents and related software. Responsible for configuration status accounting. Tracks all problems and changes in product documents and reports changes and current configuration. Responsible for configuration audits. Supports audits to verify that requirements of all baselines have been met. Supports quality assurance process audits. Develops release and rollout plans and schedules.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate's degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Database Management Specialist

Minimum Experience/General Experience: Four years of experience in a related field.

Functional Responsibility: Responsible for all activities related to the administration of computerized databases. Assigns personnel to various projects and directs their activities. Reviews and evaluates work and prepares performance reports. Confers with and advises subordinates on administrative policies and procedures, technical problems, priorities, and methods. Consults with and advises users of various databases. Projects long-range requirements for database administration in conjunction with other managers in the information systems function as well as business function managers. Prepares activity and progress reports regarding database management.

Minimum Education:
- Bachelors degree in degree in a technical or engineering discipline.
• An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.

• Masters degree may be substituted for 2 years of experience.

• Doctorate may be substituted for 4 years of experience.

Developer I
Minimum Experience/General Experience: Six years of experience on a technical development team in the areas of software and application development. Familiarity with standard concepts, practices, and procedures within the area of technical development. Knowledge of full cycle software development and relational database concepts.

Functional Responsibility: Designs, modifies, develops, writes, and implements software programming applications. Supports and/or installs software applications. Participates in the testing process through test review and analysis, test witnessing, and certification of software. Relies on experience and judgment to plan and accomplish goals. Performs a variety of tasks.

Minimum Education:
• Bachelors degree.
• Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Developer II
Minimum Experience/General Experience: Eight years of experience on a technical development team in the areas of software and application development. Familiarity with standard concepts, practices, and procedures within the area of technical development. Knowledge of full cycle software development and relational database concepts.

Functional Responsibility: Designs, modifies, develops, writes, and implements software programming applications. Supports and/or installs software applications. Participates in the testing process through test review and analysis, test witnessing, and certification of software. Relies on experience and judgment to plan and accomplish goals. Leads development efforts on moderately complex applications. Performs a variety of tasks.

Minimum Education:
• Bachelors degree.
• Masters degree may be substituted for 2 years of experience.

Developer III
Minimum Experience/General Experience: Ten or more years of experience on a technical development team in the areas of software and application development. Familiarity with standard concepts, practices, and procedures within the area of technical development. Knowledge of full cycle software development and relational database concepts.

Functional Responsibility: Designs, modifies, develops, writes, and implements software programming applications. Supports and/or installs software applications. Participates in the testing process through test review and analysis, test witnessing, and certification of software. Relies on experience and judgment to plan and accomplish goals. Leads development efforts on moderately complex to complex applications. Performs a variety of tasks.

Minimum Education:
• Bachelors degree.
• Masters degree may be substituted for 2 years of experience.
• Doctorate may be substituted for 4 years of experience.
IT Security Analyst
Minimum Experience/General Experience: Four years of experience in a related field. May have expert credentials or be recognized as an authority.

Functional Responsibility: Designs, develops, engineers and implements solutions to security requirements. Performs risk analyses which also includes risk assessment. Assists with coordination and implementation of the organization’s information security. A working knowledge of several of the following areas is required: understanding of business security practices and procedures; knowledge of current security tools available; hardware/software security implementation; different communication protocols; encryption techniques/tools; familiarity with commercial products; and, current Internet technology

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Lead Technical Developer
Minimum Experience/General Experience: Eight years of experience on a technical development team in the areas of software and application development. Familiarity with a variety of the field’s concepts, practices, and procedures. Expertise with software development and relational database knowledge.

Functional Responsibility: Design, modify, develop, write, and implement software programming applications. Support and/or install software applications. Participate in the testing process through test review and analysis, test witnessing, and certification of software. Manage a team of software developers to architect and design enterprise software products. Write product requirement documents, implement and track development timelines, negotiate feature sets with the development leads. Relies on experience and judgment to plan and accomplish goals. Performs a variety of complicated tasks.

Minimum Education:
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Network Administrator
Minimum Experience/General Experience: Two years of experience in a related field.

Functional Responsibility: Under general supervision, responsible for the acquisition, installation, maintenance, and usage of the organization’s local area network (LAN). Manages LAN performance and maintains LAN security. Ensures that security procedures are implemented and enforced. Installs all network hardware and software. Evaluates, develops, and maintains telecommunications systems. Troubleshoots LAN problems. Establishes and implements LAN policies, procedures, and standards and ensures their conformance with information systems and organization objectives. Trains users on LAN operation. Frequently reports to a PC support manager or Senior LAN Administrator.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.
Network Engineer
Minimum Experience/General Experience: Four years of experience in a related field.

Functional Responsibility: Under general supervision, oversees the purchase, installation, and support of network communications, including LAN/WAN systems. Works on problems of diverse scope where analysis of situation requires evaluation and judgment. Responsible for evaluating current systems. Assists in the planning of large-scale systems projects through vendor comparison and cost studies. Requires thorough knowledge of LAN/WAN systems, networks, and applications.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Packaged Software Consultant I
Minimum Experience/General Experience: Two years of experience in implementing packaged software applications or hands-on experience with packaged software applications. Familiarity with relational database concepts and client-server architectures.

Functional Responsibility: Under direct supervision, reviews, analyzes, and modifies packaged software systems including encoding, testing, debugging, and installing to support an organization’s applications systems. May be expected to write documentation to describe program development, logic, coding, and corrections. Writes manual for users to describe installation and operating procedures.

Minimum Education:
- Bachelors degree.
- Masters degree may be substituted for 2 years of experience.

Packaged Software Consultant II
Minimum Experience/General Experience: Five years of experience in implementing packaged software applications or hands-on experience with packaged software applications. Familiarity with relational database concepts and client-server architectures. Relies on experience and judgment to plan and accomplish goals.

Functional Responsibility: Reviews, analyzes, and modifies packaged software systems including encoding, testing, debugging, and installing to support an organization’s applications systems. Consults with users to identify current operating procedures and to clarify program objectives. May be expected to write documentation to describe program development, logic, coding, and corrections. Writes manual for users to describe installation and operating procedures.

Minimum Education:
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Packaged Software Consultant III
Minimum Experience/General Experience: Seven years of experience in implementing packaged software applications or hands-on experience with packaged software applications. Expertise with relational database concepts and client-server architectures. Relies on experience and judgment to plan and accomplish goals.

Functional Responsibility: Reviews, analyzes, and modifies packaged software systems including encoding,
testing, debugging, and installing to support an organization’s applications systems. Consults with users to identify current operating procedures and to clarify program objectives. Writes documentation to describe program development, logic, coding, and corrections. Writes manuals for users to describe installation and operating procedures.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Program Manager
Minimum Experience/General Experience: Six years experience in a management or technical role.

Functional Responsibility: Organizes, directs, and coordinates planning and production of all the program support activities. Demonstrated experience for oral and written communications with all levels of management for planning and control of projects. Interfaces with customer management personnel, customer contracts staff, and other cognizant customer officials.

Formulates and reviews project plans, determines cost, and ensures conformance to work standards. Responsible for formulating and enforcing work standards, assigning contractor schedules, reviewing work discrepancies, supervising contractor personnel and communicating policies, purposes, and goals of the organization to subordinates. Assigns, schedules, and reviews work of subordinates. Able to evaluate proposed information systems to determine technical feasibility with government specified technologies, cost for implementation and operation, as well as functional adequacy.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Project Manager II
Minimum Experience/General Experience: Four years of experience required specializing in management, resource allocation, or information technology, including full cycle software/web development and/or implementation knowledge.

Functional Responsibility: Manage projects, tasks, and/or subtasks. Advise and assist project staff on execution of specific project requirements. May be responsible for management of complete project or specific task elements. Implements directives and schedules necessary to ensure effective project management. Possesses a detailed knowledge of concepts, practices, and procedures in several activity, technical, and management fields.

Minimum Education:
- Bachelors degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Project Manager III
Minimum Experience/General Experience: Nine years of experience required specializing in management, resource allocation, or information technology, including full cycle software/web development and/or implementation expertise.
Functional Responsibility: Manage projects, tasks, and/or subtasks. Advise and assist project staff on execution of specific project requirements. May be responsible for management of complete project or specific task elements. Implements directives and schedules necessary to ensure effective project management. Possesses a detailed knowledge of concepts, practices, and procedures in several activity, technical, and management fields. Provides technical consulting on complex projects and provides detailed guidance and direction to project staff.

Minimum Education:
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

Subject Matter Expert (SME) I
Minimum Experience/General Experience: Five years of experience in a related field.

Functional Responsibility: Provides expert support, analysis, and research into especially complex problems and processes under broad direction. Provides technical direction, interprets requirements, and performs analysis of alternatives. Thinks independently and demonstrates superior written and oral communications skills. Possesses a complete understanding and wide experience in the application of relevant principles, theories, and concepts. Independently develops solutions. Expertise is in a particular domain or area of Information Technology.

Minimum Education:
- Bachelors degree.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.

Subject Matter Expert (SME) II
Minimum Experience/General Experience: Four years of experience in a related field.

Functional Responsibility: Provides expert support, analysis, and research into exceptionally complex problems and processes with minimal direction. Provides technical direction, interprets requirements, and performs analysis of alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. May function in a leadership role. Possesses expertise and wide experience in the application of relevant principles, theories, and concepts. Solves complex problems that require the regular use of ingenuity and creativity. Expertise is in a particular domain or area of Information Technology.

Minimum Education:
- Bachelors degree.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Subject Matter Expert (SME) III
Minimum Experience/General Experience: Seven years of experience in a related field.

Functional Responsibility: Provides expert support, analysis, and research into exceptionally complex problems and processes. Serves as technical expert providing technical direction, interprets requirements, and performs analysis of alternatives. Thinks independently and demonstrates exceptional written and oral communications skills. Understands and applies advanced principles, theories, and concepts. May function in a leadership role. Solves exceptionally complex problems that require solutions which are highly innovative. Expertise is in a
particular domain or area of Information Technology.

**Minimum Education:**
- Bachelors degree.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor’s degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

**Systems Engineer**

**Minimum Experience/General Experience:** Four years of experience in a related field.

**Functional Responsibility:** Analyzes functional business requirements and design specifications for functional activities. Should provide identification/fixing for the problems within existing systems design/implementation of new systems, enhances the existing systems, and participates in analysis, design, and new construction of next generation IT systems.

Responsible for understanding the needs of the customers and the realities of commercially available IT products, and creating requirements that will allow implementation by the architecture and engineering team and COTS products. Must possess experience of system engineering in one or more areas including telecommunications concepts, computer languages, operating systems, database/DBMS and middleware.

**Minimum Education:**
- Bachelors degree.
- Masters degree or specialized experience in the technologies that meet the specific statement of work for the services to be provided may be substituted for years of experience.

**Technical Architect I**

**Minimum Experience/General Experience:** Five years of experience supporting efforts to design architectures to include the software, hardware, and communications to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces.

**Functional Responsibility:** Establishes system information requirements in the development of enterprise-wide or large-scale information systems. Contributes to technical design, product and vendor selection, application and technical architectures. Provides subject matter expertise on various technologies and platforms. Ensures that the systems are compatible and in compliance with the industry standards, best practices, and client requirements. Ensures that the common operating environment is compliant with all security and architecture standards, evaluates analytically and systematically problems of workflows, organization, and plans, and develops appropriate corrective action.

**Minimum Education:**
- Bachelors degree.

**Technical Architect II**

**Minimum Experience/General Experience:** Eight years of experience supporting efforts to design architectures to include the software, hardware, and communications to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces. This individual has experience analyzing processes, translating requirements to technical requirements, and providing technology expertise.

**Functional Responsibility:** Establishes system information requirements in the development of enterprise-wide or large-scale information systems. Contributes to technical design, product and vendor selection, application and technical architectures. Provides subject matter expertise on various technologies and platforms. Ensures that the systems are compatible and in compliance with the industry standards, best practices, and client requirements. Ensures that the common operating environment is compliant with all security and architecture standards, evaluates analytically and systematically problems of workflows, organization, and plans, and develops appropriate corrective action.
standards, evaluates analytically and systematically problems of workflows, organization, and plans, and develops appropriate corrective action.

Minimum Education:

- Bachelors degree.

**Technical Architect III**

Minimum Experience/General Experience: Ten years of experience supporting efforts to design architectures to include the software, hardware, and communications to support the total requirements, as well as provide for present and future cross-functional requirements and interfaces. This individual has extensive experience analyzing processes, translating requirements to technical requirements, and providing technology expertise.

Functional Responsibility: Establishes system information requirements in the development of enterprise-wide or large-scale information systems. Contributes to technical design, product and vendor selection, application, and technical architectures. Provides subject matter expertise on various technologies and platforms. Ensures that the systems are compatible and in compliance with the industry standards, best practices, and client requirements. Ensures that the common operating environment is compliant with all security and architecture standards, evaluates analytically and systematically problems of workflows, organization, and plans, and develops appropriate corrective action.

Minimum Education:

- Bachelors degree
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

**Tester – Performance**

Minimum Experience/General Experience: Four years of software testing experience.

Functional Responsibility: Performs and leads processes related to testing activities for new software development systems and applications. Responsible for developing and executing formal test plans to ensure the delivery of quality software applications. Serves as a mentor to lower level testing analysts and may provide work direction to others in project team(s). Familiarity with performance testing.

Minimum Education:

- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate's degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

**Tester I**

Minimum Experience/General Experience: Two years of software testing experience.

Functional Responsibility: Under direct supervision, performs analysis of documented user requirements and assists in the design of test plans in support of user requirements for moderately complex to complex software or IT systems. Reviews system requirements documentation; designs, defines and documents unit and application test plans; transforms test plans into test scripts and executes those scripts. May participate in all phases of risk management assessment and software/hardware development under the direction of a Senior Test Engineer. Responsible for documentation of test results in test logs or defect tracking systems. Responsible for verifying that the test designs and documentation support all applicable client, agency, or industry standards, time lines, and budgets. Develops test data to be used in performing the required tests. Assists in the analysis of test results, documents conclusions and makes recommendations as supported by such analysis.
Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.

Tester II
Minimum Experience/General Experience: Four years of software testing experience.

Functional Responsibility: Performs analysis of documented user requirements and directs or assists in the design of test plans in support of user requirements for moderately complex to complex software or IT systems. Reviews user application system requirements documentation; designs, defines and documents unit and application test plans; transforms test plans into test scripts and executes those scripts. May participate in all phases of risk management assessment and software/hardware development under the direction of a Senior Test Engineer. Responsible for ensuring proper execution of test scripts and documentation of test results in test logs or defect tracking systems. Responsible for ensuring that the test designs and documentation support all applicable client, agency or industry standards, time lines and budgets. Responsible for the development of test data to be used in performing the required tests. Responsible that testing conclusions and recommendations are fully supported by test results, and that project managers are fully informed of testing status and application deviations from documented user requirements. Responsible for/assists in the analysis of test results, documents conclusions, and makes recommendations as supported by such analysis.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Web Designer
Minimum Experience/General Experience: Four years of related experience.

Functional Responsibility: Designs and builds web pages using a variety of graphics software applications, techniques, and tools. Designs and develops user interface features, site animation, and special effects elements. Contributes to the design group’s efforts to enhance the appeal of the organization’s online offerings. Designs the website to support the organization’s strategies and goals relative to external communications. Typically requires one to three years of experience in the area of web design. Requires knowledge of web-based technologies including browsers ASP pages, HTML code, object-oriented technology, and graphics software.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Web Developer I
Minimum Experience/General Experience: Two years of related experience.

Functional Responsibility: Under direct supervision, designs, develops, troubleshoots, debugs, and implements
software code (such as HTML, CGI, and JavaScript) for a component of the website. Integrates web applications with backend databases. Deploys large web-based transaction systems using application servers. Tests, builds, and coordinates the integration of new products per production and client requirements. Requires strong navigation and site-design instincts.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.

Web Developer II
Minimum Experience/General Experience: Four years of related experience.

Functional Responsibility: Under general supervision, designs, develops, troubleshoots, debugs, and implements software code (such as HTML, CGI, and JavaScript) for a component of the website. Works with graphic designers and other members of a project team to develop the site concept, interface design, and architecture of the website. Responsible for interface implementation. Integrates web applications with backend databases. Deploys large web-based transaction systems using application servers. Researches, tests, builds, and coordinates the integration of new products per production and client requirements. Requires strong navigation and site-design instincts.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.

Web Developer III
Minimum Experience/General Experience: Six years of related experience.

Functional Responsibility: Leads design, development, troubleshooting, debugging, and implementation of software code (such as HTML, CGI, and JavaScript) for a component of the website. Works with graphic designers and other members of a project team to develop the site concept, interface design, and architecture of the website. Responsible for interface implementation. Integrates web applications with backend databases. Deploys large web-based transaction systems using application servers. Researches, tests, builds, and coordinates the integration of new products per production and client requirements. Requires strong navigation and site-design instincts.

Minimum Education:
- Bachelors degree in a technical or engineering discipline.
- An additional four (4) years of experience and an Associate’s degree or an additional 8 years of experience and a high school diploma or GED may be substituted for a Bachelor's degree.
- Masters degree may be substituted for 2 years of experience.
- Doctorate may be substituted for 4 years of experience.
## GSA IT SERVICES PRICELIST

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>GSA Rate with IFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>518210C</td>
<td>Cloud Architect Level I</td>
<td>$ 126.12</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Architect Level II</td>
<td>$ 159.64</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Architect Level III</td>
<td>$ 195.12</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Analyst Level I</td>
<td>$ 97.95</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Analyst Level II</td>
<td>$ 112.16</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Analyst Level III</td>
<td>$ 129.99</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Operations Analyst Level I</td>
<td>$ 97.95</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Operations Analyst Level II</td>
<td>$ 129.99</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Operations Analyst Level III</td>
<td>$ 179.99</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Site Reliability Engineer Level I</td>
<td>$ 129.11</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Site Reliability Engineer Level II</td>
<td>$ 145.78</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Site Reliability Engineer Level III</td>
<td>$ 179.42</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Engineer Level II</td>
<td>$ 158.74</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Engineer Level III</td>
<td>$ 193.57</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Migration Specialist Level I</td>
<td>$ 129.11</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Migration Specialist Level II</td>
<td>$ 145.78</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Migration Specialist Level III</td>
<td>$ 179.42</td>
</tr>
<tr>
<td>518210C</td>
<td>Azure/Google/AWS Cloud Security Engineer Level I</td>
<td>$ 142.92</td>
</tr>
<tr>
<td>518210C</td>
<td>Azure/Google/AWS Cloud Security Engineer Level II</td>
<td>$ 154.13</td>
</tr>
<tr>
<td>518210C</td>
<td>Azure/Google/AWS Cloud Security Engineer Level III</td>
<td>$ 166.22</td>
</tr>
<tr>
<td>518210C</td>
<td>IT Cloud Subject Matter Specialist Level I</td>
<td>$ 118.27</td>
</tr>
<tr>
<td>518210C</td>
<td>IT Cloud Subject Matter Specialist Level II</td>
<td>$ 176.57</td>
</tr>
<tr>
<td>518210C</td>
<td>IT Cloud Subject Matter Specialist Level III</td>
<td>$ 261.65</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Security Information Assurance Engineer Level II</td>
<td>$ 176.57</td>
</tr>
<tr>
<td>518210C</td>
<td>Cloud Security Information Assurance Engineer Level III</td>
<td>$ 261.65</td>
</tr>
</tbody>
</table>

### Year 11 - Year 15

<table>
<thead>
<tr>
<th>SIN</th>
<th>Labor Category</th>
<th>Year 11</th>
<th>Year 12</th>
<th>Year 13</th>
<th>Year 14</th>
<th>Year 15</th>
</tr>
</thead>
<tbody>
<tr>
<td>54151HACS</td>
<td>Chief Cyber Information Security Officer</td>
<td>May 1, 2019 - April 30, 2020</td>
<td>$ 261.65</td>
<td>$ 266.88</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Chief Cyber Information Security Officer - Deputy</td>
<td>May 1, 2020 - April 30, 2021</td>
<td>$ 176.57</td>
<td>$ 180.11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist Level I</td>
<td>May 1, 2021 - April 30, 2022</td>
<td>$ 107.65</td>
<td>$ 109.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist Level II</td>
<td>May 1, 2022 - April 30, 2023</td>
<td>$ 132.53</td>
<td>$ 135.18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Specialist Level III</td>
<td>May 1, 2023 - April 30, 2024</td>
<td>$ 151.85</td>
<td>$ 154.88</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Data Scientist/Cyber Data Analyst</td>
<td>May 1, 2024 - April 30, 2025</td>
<td>$ 164.59</td>
<td>$ 167.89</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Information Security Analyst Level I</td>
<td>May 1, 2026 - April 30, 2027</td>
<td>$ 92.54</td>
<td>$ 94.40</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Information Security Analyst Level II</td>
<td>May 1, 2028 - April 30, 2029</td>
<td>$ 117.41</td>
<td>$ 119.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Information Security Analyst Level III</td>
<td>May 1, 2030 - April 30, 2031</td>
<td>$ 136.74</td>
<td>$ 139.47</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIN</td>
<td>Labor Category</td>
<td>Year 11 (May 1, 2019 - April 30, 2020)</td>
<td>Year 12 (May 1, 2020 - April 30, 2021)</td>
<td>Year 13 (May 1, 2021 - April 30, 2022)</td>
<td>Year 14 (May 1, 2022 - April 30, 2023)</td>
<td>Year 15 (May 1, 2023 - April 30, 2024)</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Information Assurance Engineer Level I</td>
<td></td>
<td></td>
<td></td>
<td>$161.20</td>
<td>$164.42</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Information Assurance Engineer Level II</td>
<td></td>
<td></td>
<td></td>
<td>$179.34</td>
<td>$182.92</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Information Assurance Engineer Level III</td>
<td></td>
<td></td>
<td></td>
<td>$193.57</td>
<td>$197.44</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Windows Cyber System Security Engineer Level I</td>
<td></td>
<td></td>
<td></td>
<td>$112.69</td>
<td>$114.94</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Windows Cyber System Security Engineer Level II</td>
<td></td>
<td></td>
<td></td>
<td>$137.57</td>
<td>$140.32</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Windows Cyber System Security Engineer Level III</td>
<td></td>
<td></td>
<td></td>
<td>$156.89</td>
<td>$160.02</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Penetration Tester Level I</td>
<td>$92.54</td>
<td>$94.40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Penetration Tester Level II</td>
<td>$117.41</td>
<td>$119.76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Penetration Tester Level III</td>
<td>$136.74</td>
<td>$139.47</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Threat Intelligence Analyst Level I</td>
<td>$79.02</td>
<td>$80.60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Threat Intelligence Analyst Level II</td>
<td>$108.68</td>
<td>$110.85</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Threat Intelligence Analyst Level III</td>
<td>$121.93</td>
<td>$124.37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Tools Engineer/Cyber Engineering Subject Matter Specialist Level II</td>
<td></td>
<td></td>
<td></td>
<td>$176.57</td>
<td>$180.11</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Tools Engineer/Cyber Engineering Subject Matter Specialist Level III</td>
<td></td>
<td></td>
<td></td>
<td>$261.65</td>
<td>$266.88</td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level I</td>
<td>$65.43</td>
<td>$66.74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level II</td>
<td>$94.24</td>
<td>$96.12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Security Code Reviewers/Cyber Information Assurance Engineer Level III</td>
<td>$121.45</td>
<td>$123.88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Vulnerability Analyst Level I</td>
<td>$79.02</td>
<td>$80.60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Vulnerability Analyst Level II</td>
<td>$108.68</td>
<td>$110.85</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber Vulnerability Analyst Level III</td>
<td>$121.93</td>
<td>$124.37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber SOC Analyst Level I</td>
<td>$79.02</td>
<td>$80.60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber SOC Analyst Level II</td>
<td>$108.68</td>
<td>$110.85</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber SOC Analyst Level III</td>
<td>$121.93</td>
<td>$124.37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber SIEM Engineer Level I</td>
<td>$92.54</td>
<td>$94.40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HACS</td>
<td>Cyber SIEM Engineer Level II</td>
<td>$117.41</td>
<td>$119.76</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Application Engineer I</td>
<td>$113.00</td>
<td>$115.26</td>
<td>$117.56</td>
<td>$119.92</td>
<td>$122.31</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Business Analyst</td>
<td>$148.51</td>
<td>$151.48</td>
<td>$154.51</td>
<td>$157.60</td>
<td>$160.75</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT IM/IT I</td>
<td>$87.32</td>
<td>$89.06</td>
<td>$90.84</td>
<td>$92.66</td>
<td>$94.51</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT IM/IT II</td>
<td>$97.60</td>
<td>$99.55</td>
<td>$101.54</td>
<td>$103.57</td>
<td>$105.64</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Project Manager</td>
<td>$180.29</td>
<td>$183.90</td>
<td>$187.57</td>
<td>$191.33</td>
<td>$195.15</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Software Consultant I</td>
<td>$137.65</td>
<td>$140.41</td>
<td>$143.22</td>
<td>$146.08</td>
<td>$149.00</td>
</tr>
<tr>
<td>SIN</td>
<td>Labor Category</td>
<td>May 1, 2019 - April 30, 2020</td>
<td>May 1, 2020 - April 30, 2021</td>
<td>May 1, 2021 - April 30, 2022</td>
<td>May 1, 2022 - April 30, 2023</td>
<td>May 1, 2023 - April 30, 2024</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>54151HEAL</td>
<td>Health IT Software Consultant II</td>
<td>$169.51</td>
<td>$172.90</td>
<td>$176.36</td>
<td>$179.88</td>
<td>$183.48</td>
</tr>
<tr>
<td>54151S</td>
<td>Change, Configuration, and Release Manager</td>
<td>$131.14</td>
<td>$131.14</td>
<td>$133.76</td>
<td>$136.44</td>
<td>$139.17</td>
</tr>
<tr>
<td>54151S</td>
<td>Database Management Specialist</td>
<td>$118.61</td>
<td>$118.61</td>
<td>$120.98</td>
<td>$123.40</td>
<td>$125.87</td>
</tr>
<tr>
<td>54151S</td>
<td>Developer I</td>
<td>$136.27</td>
<td>$136.27</td>
<td>$138.99</td>
<td>$141.77</td>
<td>$144.61</td>
</tr>
<tr>
<td>54151S</td>
<td>Developer II</td>
<td>$158.80</td>
<td>$158.80</td>
<td>$161.98</td>
<td>$165.22</td>
<td>$168.52</td>
</tr>
<tr>
<td>54151S</td>
<td>Developer III</td>
<td>$164.07</td>
<td>$167.35</td>
<td>$170.70</td>
<td>$174.11</td>
<td>$177.60</td>
</tr>
<tr>
<td>54151S</td>
<td>Financial Analyst</td>
<td>$93.56</td>
<td>$93.56</td>
<td>$95.43</td>
<td>$97.34</td>
<td>$99.28</td>
</tr>
<tr>
<td>54151S</td>
<td>IT Security Analyst</td>
<td>$135.41</td>
<td>$135.41</td>
<td>$138.11</td>
<td>$140.88</td>
<td>$143.69</td>
</tr>
<tr>
<td>54151S</td>
<td>Lead Technical Developer</td>
<td>$152.62</td>
<td>$152.62</td>
<td>$155.68</td>
<td>$158.79</td>
<td>$161.97</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Administrator</td>
<td>$75.01</td>
<td>$75.01</td>
<td>$76.52</td>
<td>$78.05</td>
<td>$79.61</td>
</tr>
<tr>
<td>54151S</td>
<td>Network Engineer</td>
<td>$94.71</td>
<td>$94.71</td>
<td>$96.61</td>
<td>$98.54</td>
<td>$100.51</td>
</tr>
<tr>
<td>54151S</td>
<td>Packaged Software Consultant I</td>
<td>$112.49</td>
<td>$114.74</td>
<td>$117.03</td>
<td>$119.37</td>
<td>$121.76</td>
</tr>
<tr>
<td>54151S</td>
<td>Packaged Software Consultant II</td>
<td>$145.17</td>
<td>$148.07</td>
<td>$151.03</td>
<td>$154.05</td>
<td>$157.14</td>
</tr>
<tr>
<td>54151S</td>
<td>Program Manager</td>
<td>$180.93</td>
<td>$184.55</td>
<td>$188.24</td>
<td>$192.00</td>
<td>$195.85</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager II</td>
<td>$132.55</td>
<td>$135.20</td>
<td>$137.90</td>
<td>$140.66</td>
<td>$143.47</td>
</tr>
<tr>
<td>54151S</td>
<td>Project Manager III</td>
<td>$161.52</td>
<td>$164.75</td>
<td>$168.05</td>
<td>$171.41</td>
<td>$174.84</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert (SME) I</td>
<td>$208.69</td>
<td>$212.86</td>
<td>$217.12</td>
<td>$221.46</td>
<td>$225.89</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert (SME) II</td>
<td>$245.24</td>
<td>$245.24</td>
<td>$250.15</td>
<td>$255.15</td>
<td>$260.25</td>
</tr>
<tr>
<td>54151S</td>
<td>Subject Matter Expert (SME) III</td>
<td>$284.40</td>
<td>$284.40</td>
<td>$290.09</td>
<td>$295.89</td>
<td>$301.81</td>
</tr>
<tr>
<td>54151S</td>
<td>Systems Engineer</td>
<td>$114.25</td>
<td>$114.25</td>
<td>$116.54</td>
<td>$118.87</td>
<td>$121.25</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Architect I</td>
<td>$142.66</td>
<td>$145.52</td>
<td>$148.43</td>
<td>$151.40</td>
<td>$154.42</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Architect II</td>
<td>$174.43</td>
<td>$174.43</td>
<td>$177.92</td>
<td>$181.48</td>
<td>$185.11</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Architect III</td>
<td>$181.67</td>
<td>$185.30</td>
<td>$189.00</td>
<td>$192.78</td>
<td>$196.64</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Business Analyst I</td>
<td>$90.52</td>
<td>$92.33</td>
<td>$94.17</td>
<td>$96.06</td>
<td>$97.98</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Business Analyst II</td>
<td>$112.16</td>
<td>$112.16</td>
<td>$114.40</td>
<td>$116.69</td>
<td>$119.02</td>
</tr>
<tr>
<td>54151S</td>
<td>Technical Business Analyst III</td>
<td>$121.88</td>
<td>$124.32</td>
<td>$126.80</td>
<td>$129.34</td>
<td>$131.93</td>
</tr>
<tr>
<td>54151S</td>
<td>Tester – Performance</td>
<td>$216.50</td>
<td>$216.50</td>
<td>$220.83</td>
<td>$225.25</td>
<td>$229.75</td>
</tr>
<tr>
<td>54151S</td>
<td>Tester I</td>
<td>$85.53</td>
<td>$85.53</td>
<td>$87.24</td>
<td>$88.99</td>
<td>$90.77</td>
</tr>
<tr>
<td>54151S</td>
<td>Tester II</td>
<td>$93.01</td>
<td>$94.87</td>
<td>$96.77</td>
<td>$98.70</td>
<td>$100.68</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Designer</td>
<td>$109.28</td>
<td>$109.28</td>
<td>$111.46</td>
<td>$113.69</td>
<td>$115.97</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Developer I</td>
<td>$95.92</td>
<td>$97.84</td>
<td>$99.80</td>
<td>$101.79</td>
<td>$103.83</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Developer II</td>
<td>$121.76</td>
<td>$124.19</td>
<td>$126.67</td>
<td>$129.21</td>
<td>$131.79</td>
</tr>
<tr>
<td>54151S</td>
<td>Web Developer III</td>
<td>$148.65</td>
<td>$148.65</td>
<td>$151.63</td>
<td>$154.66</td>
<td>$157.75</td>
</tr>
</tbody>
</table>
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

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

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

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

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

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

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

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

John Noh, Chief Financial Officer
Phone: 703-639-1918
E-mail: jnoh@collabralink.com
(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and CollabraLink Technologies, Inc. enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract GS-35F-0398V.

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

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

Signatures

Ordering Activity        Date    CollabraLink Technologies, Inc.        Date
Pursuant to GSA Federal Supply Schedule Contract Number GS-35F-0398V, Blanket Purchase Agreements, CollabraLink Technologies, Inc. agrees to the following terms of a Blanket Purchase Agreement (BPA)

EXCLUSIVELY WITH (ordering activity):

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

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

(2) Delivery:

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

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

(4) This BPA does not obligate any funds.

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

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

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

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

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

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

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

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor's invoice, the provisions of this BPA will take precedence.
Federal Supply Schedule Contractors may use “Contractor Team Arrangements” (see FAR 9.6) to provide solutions when responding to a ordering activity requirements.

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

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

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

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

Here is a general outline on how it works:

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