AUTHORIZED FEDERAL SUPPLY SERVICE MASS
CONSOLIDATED SOLICITATION PRICE LIST
GENERAL PURPOSE INFORMATION TECHNOLOGY SERVICES

Komplete Systems Integrators, Inc.
12057 Olmstead Dr
Fayetteville GA 30215-6640
Office Phone: (770) 690-4272
Mobile Phone 24/7: (678) 362-2911
Fax: (770) 460-2062
www.kompsys.com

Contract Number: 47QTCA20D00DQ
Period Covered by Contract: August 12, 2020 through August 11, 2025

General Services Administration
Federal Acquisition Service

Pricelist current through Modification # 0005, dated November 09, 2020.

All IT Professional Services and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System (http://www.gsaadvantage.gov).

CUSTOMER INFORMATION:

1. Awarded Special Item Number(s):

SIN	Description
54151S	Information Technology Professional Services – Subject to Cooperative Purchasing
518210C	Cloud and Cloud-Related IT Professional Services – Subject to Cooperative Purchasing
54151HACS	Highly Adaptive Cybersecurity Services (HACS)
OLM	Order Level Materials

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

Job Title / Task	Labor Category Description	GSA Hourly Rate
Help Desk III	**Serves as a point of escalation for troubleshooting hardware, software, PC and printer problems. Functional Responsibility: Serves as a technical lead in a helpdesk environment highly skilled at troubleshooting software and network issues demonstrates fault isolation and restoral techniques to resolve end user issues.**	**$54.35**

1c. Labor Category Descriptions of all corresponding commercial job titles, experience, functional responsibility and education are outlined on Pages 8 - 9 & 34 – 35 within this pricelist.

2. Maximum Order for each SIN:

SIN#	MAXIMUM ORDER
54151S	**$500,000.00 USD**
518210C	**$500,000.00 USD**
54151HACS	**$500,000.00 USD**

3. Minimum Order: $100.00 USD

4. Geographic Scope of Coverage: The Geographic Scope of Coverage is Domestic: V – 48 States

& DC.

5. **Point(s) of production:** Not Applicable We are Offering Services Only

6. **Discount:** Prices listed within this price list are net prices.

7. **Quantity Discounts:** Additional 1% Discount on Orders $500,001.00 - $999,999.99; Additional 2% Discount on Orders Exceeding $1 Million.

8. **Prompt Payment Terms:** Net 15 1.00% , Net 30 0.00%

9. **Government Purchase Cards:** Government Purchase Cards are accepted at, below, and above the micro-purchase thresholds.

10. **Foreign Items:** Not Applicable We are Offering Services Only

11. **Normal Delivery Terms:** Determined At Task Order Level. Please contact Contractor.

11b. **Expedited Delivery Terms:** Determined At Task Order Level. Please contact Contractor.

11c. **Overnight/2-Day Delivery Terms:** Determined At Task Order Level. Please contact Contractor.

11d. **Urgent Requirements:** Determined At Task Order Level. Please contact Contractor.

12. **FOB Point:** Not Applicable Offering Services Only

13. **Ordering Address:** **Komplete Systems Integrators, Inc.**
12057 Olmstead Dr
Fayetteville GA 30215-6640

13b. Ordering Procedures for Federal Supply Schedule Contracts: Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405-3 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.

14. **Payment Address:** **Komplete Systems Integrators, Inc.**
12057 Olmstead Dr
Fayetteville GA 30215-6640

15. **Warranty/Guarantee Provisions:** Standard Service Warranty.

16. **Export Packing Charges:** Not Applicable; Offering Services Only.

17. **Terms & Conditions of Government Purchase Card Acceptance:** Government Purchase card is accepted at, above, and below the micro purchase threshold with no additional thresholds identified at this time.

18. **Terms and Conditions of Rental, Maintenance, and Repair:** Not Applicable.

19. **Terms and Conditions For Installation:** Not Applicable.

20. Terms and Conditions of Repair Parts: Not Applicable.

20a. Terms and Conditions For Any Other Services: Not Applicable.

21. List of Service & Distribution Points: Not Applicable.

22. List of Participating Dealers: Not Applicable.

23. Preventative Maintenance : Not Applicable.

24. Special Attributes: Not Applicable

25. Data Universal Number System (DUNS) Number: 076363527

26. Notification Regarding Registration in System For Award Management (SAM) Database: Komplete Systems Integrators, Inc. is Currently and accurately registered and up to date.

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBERS 54151S)

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

1. SCOPE

a. The prices, terms and conditions stated under Special Item Numbers 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.

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

2. PERFORMANCE INCENTIVES I-FSS-60 Performance Incentives (April 2000)

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

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

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

3. ORDER

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

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

4. PERFORMANCE OF SERVICES

a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.

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

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

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

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

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

(1) Cancel the stop-work order; or

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

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

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

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

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

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

6. INSPECTION OF SERVICES

In accordance with FAR 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR

2009) (DEVIATION I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 CONTRACT TERMS AND CONDITIONS COMMERCIAL ITEMS (MAR 2009) (ALTERNATE I OCT 2008) (DEVIATION I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

7. RESPONSIBILITIES OF THE CONTRACTOR

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

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT Professional Services.

9. INDEPENDENT CONTRACTOR

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

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

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

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

11. INVOICES

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

12. PAYMENTS

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

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

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

(1) The offeror;

(2) Subcontractors; and/or

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

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

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

15. APPROVAL OF SUBCONTRACTS

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING: SIN 54151S

IT PROFESSIONAL SERVICES RATES

SIN 54151S

Labor Category / Service Proposed	GSA Rate Including IFF
Project Manager	$134.40
Enterprise Architect	$155.46
Computer Telephony Integration Architect	$155.46
Network Engineer	$136.48
Field Technician	$74.56
Help Desk Supervisor	$64.74
Help Desk III	$54.76
Technical Writer **	$64.74

Labor Category Descriptions: SIN 54151S

Title: Project Manager
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree, Project Manager Certification**
Responsibilities:

The IT project manager is responsible for the planning, organization, project budgeting, resource management, and discipline pertaining to the successful completion of a specific information system project. Maintains and tracks scheduled events and project milestones. Provides leadership to the project staff, and responsible to resolve client escalations.

Title: Enterprise Architect
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Works with customers to analyze needs, design solutions to support business requirements.

Title: Computer Telephony Integration Architect
Minimum Year Experience: **8 Years**
Minimum Education: **PhD in Computer Science, Electrical or Electronics Engineering**
Responsibilities:

The IP Telephony expert is responsible for network discovery/design and assessment, network traffic analysis, impact analysis, topology design and network performance tuning. Has a full understanding of H.323 and or MGCP, VoIP server implementation, understands dial plans and 911 deployment requirements. or higher. Evaluates the impact of proposed solutions onto the network and be responsible for any lower layer modifications to the infrastructure (QoS, Routing, Switching, etc.). The IP Telephony expert requires specific training requirements to support scalable solutions.

Title: Network Engineer
Minimum Year Experience: 6 **Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Experienced with data network design, device configuration, installation and troubleshooting in IP routed

networks, Frame Relay, ATM and SONET networks. Experience may include core backbones to edge tail sites. Skilled in maintaining and troubleshooting large Corporate Enterprise environments as well as Inter-regional Service Provider environments. Network device knowledge should include routers, switches, Campus ATM switches, and Wide Area ATM switches. Experience with DSL equipment, IP, VPN/MPLS, QOS. Must work well independently or as part of a group. Candidate should also be capable of managing and building multiple projects from initial conception to completion. Able to serve as area supervisor or senior level support for small groups or large Network Operations environments. Strong written communication, organizational, planning, problem solving skills; strong oral and project management skills desired.

Title: Field Technician
Minimum Year Experience: **2 Years**
Minimum Education: **High School Diploma & Microsoft Certification (MCSE); Cisco Certification Network Associate (CCNA)**
Responsibilities:

Assesses and documents current site network configuration and user requirements. Follows Direction in implementing network design plans, site installation, and Technical Design Packages. Follow's installation schedules and works with network installation team. Understands network topology and makes any configuration changes at each site. Performs post installation operations and maintenance support.

Title: Help Desk Supervisor
Minimum Year Experience: **4 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Provides daily supervision and direction to staff who are responsible for phone and in-person support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed or deployed under this contract. The personnel serve as the first point of contact for troubleshooting hardware/software, PC and printer problems. Functional Responsibility: Has the ability to design, implement and supervise employees effectively and accurately through the implementation process and support of Desktop projects. Four Years' experience managing support centers.

Title: Help Desk III
Minimum Year Experience: 4 Years
Minimum Education: Associates Degree
Responsibilities:

Serves as a point of escalation for troubleshooting hardware, software, PC and printer problems. Functional Responsibility: Serves as a technical lead in a helpdesk environment highly skilled at troubleshooting software and network issues demonstrates fault isolation and restoral techniques to resolve end user issues.

Title: Technical Writer **
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Establishes and maintains the Customer and Engineering Document Library. Sets standards for format and revision tracking for all QuickSilver documentation. Supervises and directs the work of both staff and contract technical writers. Writes technical documentation. Sets standards for and develops online help systems for QuickSilver tools. Supports and maintains the Company's third-party Customer website (Extranet). Supports day-to-day maintenance of the Company's internal website (Intranet) contents through document generation and updates. Should have 5 Yrs experience in a significant Engineering Documentation role, demonstrated authorship of technical documentation from start to finish, Demonstrated proficiency in Word, Visio, PowerPoint, Adobe Illustrator.

IT CLOUD & CLOUD-RELATED
SERVICES RATES
SIN 518210C

Labor Category / Service Proposed	GSA Rate Including IFF
Cloud Program Manager	$170.38
Cloud Project Manager	$164.44
Cloud Applications Programmer/Developer	$180.30
Cloud Architect	$175.45
Cloud Requirements Tester	$142.46

Labor Category Descriptions: SIN 518210C

Title: Cloud Program Manager
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Responsible for Cloud management, design, installation, operation and maintenance of the Cloud Technology Infrastructure. Direct all activities of cloud server, storage, network and other technologies needed for cloud success. Serve as the technical expert responsible for the design, implementation and support of cloud-based information technology solutions in current and future state. Lead the technical design, maintenance and operation of cloud-based platforms (including Azure, AWS, Google Cloud and others).

Title: Cloud Project Manager
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree, Project Manager Certification**
Responsibilities:

The Cloud Project Manager is responsible for the planning, organization, project budgeting, resource management, and discipline pertaining to the successful completion of a specific information system project within the cloud and cloud-related areas of IT. Maintains and tracks scheduled events and project milestones. Provides leadership to the project staff, and responsible to resolve client escalations.

Title: Cloud Applications Programmer/Developer
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Works with customers to design and configure software according to the customer's operations, business flow, and routing and customized management report requirements for cloud and cloud-related services and areas. In addition, designs customer reports, design and programs custom Oracle reports for all cloud and cloud-related services assigned tasks.

Title: Cloud Architect
Minimum Year Experience: **6 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Responsible for functioning as the technical delivery lead to define/document the Cloud solution architecture for software development delivery. Serves as a lead to developers to design and develop quality APIs that scale to client's environment. Write comprehensive Cloud-based technical design specifications and support documentation.

Title: Cloud Requirements Tester
Minimum Year Experience: **4 Years**
Minimum Education: **Bachelor's Degree**
Responsibilities:

Assess client's network and IT infrastructure and Cybersecurity sourcing options. Support clients in implementing and migrating to new infrastructure, cloud, network technical solutions and operational processes. Validate data and analysis for accuracy and relevance. Follow risk management and compliance procedures.

HIGHLY ADAPTIVE CYBERSECURITY (HACS) SERVICES RATES SIN 54151HACS

Labor Category / Service Proposed	GSA Rate Including IFF
Cyber Security Program Manager	$172.29
Cyber Security Project Manager	$163.22
Cyber Security Applications Programmer/Developer	$154.16
Cyber Security Architect	$154.16
Cyber Security Penetration Tester	$126.95
Cyber Security Analyst	$126.95
Cyber Security Data Analyst	$126.95
Cyber Security Privacy Officer	$145.09
Cyber Security Privacy Analyst	$126.95
Cyber Security Risk Analyst	$126.95

Labor Category Descriptions: SIN 54151HACS

Title: Cyber Security Program Manager
Minimum Year Experience: 10 Years
Minimum Education: Bachelor's Degree; Project Management Certification (PMP); Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M., or the ability to obtain this level certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:
Responsible for managing all aspects of the Cyber Security and Vulnerability Management Function. Manages a Cyber Security Program which includes the Cyber Security Project Manager and Cyber Security team responsible for Information Assurance, Vulnerability Management, Risk and Compliance and Threat Detection. Manages and supports development of security operations policies to ensure threat detection, monitoring, response, and forensics activities align with industry best practices. Works with organizations senior leadership to set direction and manage the execution of processes and procedures to evaluate and protect an organizations' security posture.

Title: Cyber Security Project Manager
Minimum Year Experience: 7 Years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M., or the ability to obtain this level certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:
The Cyber Security project manager is responsible for the planning, execution, resource management, and delivery of services in support of projects and initiatives as set forth based on the requirements of the Organization's Cybersecurity Program in accordance with industry best practices. Manages Cross functional teams and tracks scheduled events and

project milestones. Provides leadership to the project staff, and responsible to resolve client escalations.

Title: Cyber Security Applications Programmer/Developer
Minimum Year Experience: 3 Years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:
Develops Security S/W designs, reviews technical designs to identify security flaws and develops S/W to remediate. Conducts ongoing security testing, penetration testing and develops secure S/W tools and systems. Utilizes knowledge of threat vectors to understand how applications are susceptible to exploit attempts. Conducts Code and Peer reviews of technical solutions with the ability to debug and troubleshoot issues. Conduct ongoing development and testing of security solutions for patching or other preventive maintenance and hardening efforts. Participate in lifecycle development of software systems and decomposing technical requirements into function specifications. Working knowledge of such languages as Python, Java, C++, PHP and SQL

Title: Cyber Security Architect
Minimum Year Experience: 7 Years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:
Functional Responsibilities: Leads in conducting Cyber Security and information system security engineering analysis on a variety of information processing systems at various security levels. Specific knowledge includes but is not limited to; Unix, NT, MLS, and TCP/IP. Develop security accreditation/certification planning documentation. Develop security certification test plans, procedures. Conduct security certification engineering analysis and testing. Develop security risk and vulnerability assessments.

Title: Cyber Security Penetration Tester
Minimum Year Experience: 3 Years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:

Performs security tests on networks, web-based applications, and computer systems. They design tests and tools to try to break into security-protected applications and networks to probe for vulnerabilities. Remains current with the latest methods for ethical hacking and testing and always evaluating new penetration testing tools. Assess client's network and IT infrastructure and Cybersecurity sourcing options. Conducts physical assessments of servers, systems, and network device security. Searches for ways to exploit vulnerabilities and design solutions to security issues like temperature, humidity, vandalism, and natural disasters. **Conduct Security Audits** Utilizing testing methods to pinpoint ways that attackers could exploit weaknesses in security systems. One way they do this is by conducting network and system security audits, which evaluate how well an organization's system conforms to a set of established criteria. **Analyze Security Policies** Analyzes customers Security policies that identify procedures and riles for accessing and using their IT resources. these policies for effectiveness, make suggestions on security policy improvements, and work to enhance methodology material. **Write Security Assessment Reports** After conducting thorough research and testing, penetration testers document their findings, write security reports, and discuss solutions with IT teams and management. They also provide feedback and verification after security fixes are issued.

Title: Cyber Security Analyst
Minimum Year Experience: 3 years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:

Duties descriptions here. Cyber Security Analyst to support our Engineering Services Team. The contractor is responsible for planning, installing, and documenting the system's hardware and software environment; identifying areas for improvement; problem identification and resolution; and educating other support personnel. The contractor must possess the knowledge and understanding necessary for the administration of Adobe ColdFusion application framework version 8 and later, Microsoft Internet Information Services (IIS) version 6 and later, Microsoft SQL Server version 2000 and later, performing SQL code review for query optimization, and providing customers with ad hoc SQL reports. Specialized experience includes enhancing database management practices, such as implementing new database structures and formats and converting legacy data to new formats; analyzing performance data; and modifying system and database configurations to correct problems that affect the confidentiality, integrity, and availability of data. Web/Internet experience should include installing, configuring, optimizing web server and application containers. Experience and Competency with: Trusted Agent FISMA (TAF), RSA Archer or similar eGRC tools; Tenable Security Center; Strong understanding and demonstrated experience applying a risk-based approach to information security and IT assessments; Ability to work in a fast-paced, demanding environment; Excellent organizational skills and strong attention to detail; Ability to prioritize duties based on shifting demands; Strong analytical and problem-solving skills; Excellent verbal and written communication skills.

Title: Cyber Security Data Analyst
Minimum Year Experience: 3 years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:
Cybersecurity Data Analyst to perform network monitoring and vulnerability management tasks at a client site following local procedures and best practices for unclassified and classified information systems. Perform daily log review in SIEM tools of firewall, proxy, DNS (Domain Name Service), IDS (intrusion detection system), HIPS (host intrusion prevention system) logs for malicious activity. Perform daily review of all SIEM Tools notable events and alerts to review for malicious activity. Identify, develop, and tune new correlation rules in SIEM Tools to increase the amount of automated monitoring and alerts for lateral movement, privilege escalation, beaconing, persistence mechanisms, and other suspicious activity. As a subject matter expert, share and transfer knowledge to government employees to improve processes and cyber security practices. Review open vulnerabilities and research the associated CVEs (common vulnerabilities and exposures) to determine applicability and identify potential technical mitigations to reduce risk. Respond to potential cyber incidents and coordinate response actions according to Portsmouth Naval Shipyard incident response procedures. Write, update and/or modify Standard Operating Procedures (SOP's) as needed pertaining to network monitoring and incident response. Analyze threat intelligence and community data to keep abreast of security trends and make modifications to existing capabilities based on threat assessments to improve or strengthen security posture. Perform periodic audits of information system security procedures and configurations to identify deficiencies and ensure compliance with client's information system controls. Required Knowledge, Skills and Experience: SIEM Tools – Prior experience with SIEM Tools, data searches and reporting and/or Enterprise Security. Knowledge and experience creating searches, correlation rules, notables, and field extractions. Incident Response – Experience responding to suspected and confirmed network and host incidents. Knowledge and experience working through detection, analysis, containment, eradication, recovery, and remediation of incidents. Knowledge and ability to provide guidance and suggest course of actions to take in the event of an incident. Vulnerability Management – Previous experience with ACAS or Tenable Nessus Scanner. Experience evaluating vulnerabilities, assessing risk based on the environment, and identifying technical and non-technical mitigation strategies and developing mitigation statements. Event Analysis – Ability to understand and interpret Windows, UNIX OS,

firewall, web proxy, DNS, IDS, and HIPS log events. Ability to pivot between events and correlate host and network events. Understanding of Windows and UNIX event logs must be sufficient to create correlation searches for Windows and UNIX events. Minimum of one (1) years' experience working in a security operations center (SOC) environment or other network security team providing incident detection and response services utilizing a Security Information and Event Management (SIEM) At least one (1) years of experience and/or the knowledge necessary to research and mitigate vulnerabilities.

Title: Cyber Security Privacy Officer
Minimum Year Experience: 3 years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities:

Under general direction and supervision of the Privacy Officer assists with the implements an Organizational information privacy program; monitors Privacy practices in accordance with NIST Guidelines and assists with education of the HIPAA defined work force, and reviews and assimilates data on privacy uses. **Knowledge, Skills, Abilities, and Personal Characteristics:** Knowledge of privacy practices and regulatory issues impacting privacy, research, and healthcare data. Ability analyze and interpret data. Strong communication skills. Ability to maintain confidentiality. Ability to coordinate the efforts within Privacy and Compliance offices. Excellent computer skills. **Job Duties and Responsibilities**: Monitor and audit privacy practices, data use, and behavior within the enterprise. Provide advice and interpretations of policy to departments and others. Collaborate with the Privacy Officer to create reports and documentation on privacy practices. Provide education on privacy and compliance to end users; perform other duties as assigned. Support the development and implementation of privacy policies and procedures addressing privacy, confidentiality, and release of information. Identify, investigate and resolve privacy violations in the organization. Acts as the main point of contact for Privacy questions related to the Organizational Privacy Impact Assessment and associated policies.

Title: Cyber Security Privacy Analyst
Minimum Year Experience: 2 years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities**:**
Has experience in investigating privacy/security incidents and is also able to bring excellent customer services skills to the job every day. Demonstrates knowledge of privacy requirements and best practices, and understand how they apply to business practices and projects Interpret privacy requirements and best practices, and identify how they impact business projects Assess current and planned applications, systems and business processes, and identify privacy issues and design solutions for any existing gaps to ensure privacy principles, policies, practices and customer expectations Partner with business owners, technology architects, developers and product/program managers across other business units including Information Security, Technology, Operations, HR, etc. to design and develop privacy requirements and solutions across multiple technologies, platforms. Investigate actual or suspected privacy incidents independently and in partnership with other teams and communicate with leadership about reported and confirmed incidents. Experience performing privacy impact assessments (PIA) on business initiatives involving personal information (required) Experience investigating and responding to privacy incidents (required) A Bachelor's Degree in related field (preferred) 3+ years (5+ preferred) of experience working in a privacy related role Experience receiving, investigating, and responding to inquiries and requests (preferred) Strong computer skills with working proficiency in Microsoft Word, PowerPoint, Excel, and Outlook High level of personal integrity and confidentiality IAPP Certified Information Privacy Professional: CIPP/US, CIPP/C, or other IAPP credential (preferred) Prior experience and working knowledge of law and trends affecting US, Canada, and global privacy, policy and compliance including: Federal Trade Commission privacy guidance and enforcement actions, NIST, HIPAA, PIPEDA, CAN SPAM, CASL, and/or COPPA

Title: Cyber Security Risk Analyst
Minimum Year Experience: 3 years
Minimum Education: Bachelor's Degree; Information Assurance Manager (IAM) Level I certification as detailed in the Information Assurance Workforce Improvement Program (DoD 8570.01-M. The candidate must receive this certification within six months of starting this position. Security+ training qualifies for IAM Level 1 as well as other certifications listed in DoD 8570.01-M.

Responsibilities**:**
At the direction of Program Manager works with Organizational Leadership, Cybersecurity personnel, and system owners to identify security risks, conduct Risk Assessments, and quantify risk exposure and business impact of vulnerability exploitation to the organization. Duties include: Stay abreast of advances in IT concerning vulnerabilities, security breaches and attack vectors. Evaluate vulnerability data resulting from vulnerability scans, team interviews and compliance data. Evaluate security policies, processes and procedures. Examine adequacy of security control implementation and compliance. Effective communication and reporting of IT system vulnerabilities, and development of mitigation strategies. Develop cost reduction proposals for implementing preventive solutions that protect against malicious attacks or exploitation attempts. Document any gaps in security, deficiencies, security control implementation, or technical parameters such as firewall rules, encryption standards etc. Provides additional recommendations on improvements to network/application security and provides support to cross functional teams developing Root Cause Analysis, identifying threat sources, and conducting internal forensic activities.