



Authorized Price List
GSA Multiple Award Schedules (MAS) – Information Technology Professional Services

SIN 54151S / 132-51 Information Technology Professional Services

CONTRACT NUMBER – GS-35F-097DA



Contract Period – December 14, 2015 through December 13, 2025
Through Contract Mod PS-0016, dated November 10, 2021

Agil3 Technology Solutions, LLC

3141 Fairview Park Dr., Suite 315
Falls Church, VA 22042
Telephone: (703) 310-4286
Agil3 Technology Solutions, LLC (A3T) website: www.agil3tech.com

SBA Certified 8(a) Firm
SBA-Certified Small Disadvantaged Business (SDB)
Small Business
Woman Owned Business
Women Owned Small Business (WOSB)
Service-Disabled, Veteran-Owned Small Business (SDVOSB)
Economically Disadvantaged Women Owned Small Business (EDWOSB)

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 of GSA Advantage!® is:
GSAAdvantage.gov.

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



Contents

Section 1. Information for Ordering Activities	3
Section 2. A3T Labor Category Rates and Descriptions	6
Appendix A: 54151S Labor Rates and Pricing	6
Appendix B: Labor Category Descriptions	9
Section 3. Terms and Conditions	27
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S / 132-51)	27



Section 1. Information for Ordering Activities

1. Awarded SINs – 54151S / 132-51 IT Professional Services includes:

Cloud services (all associated labor);
Systems analysis, design, and implementation; and
Network services;
Cognitive computing;
Conversion and implementation support;
Database planning and design;
Internet of Things (IoT);
IT project management;
Migration services (of all kinds);
Programming;
Other services relevant to 29 CFR 541.400.

1b. Identification of the lowest priced model number and lowest unit price for that model for each special item number awarded in the contract. This price is the Government price based on a unit of one, exclusive of any quantity/dollar volume, prompt payment, or any other concession affecting price. Those contracts that have unit prices based on the geographic location of the customer, should show the range of the lowest price, and cite the areas to which the prices apply.

54151S / 132-51 **See Appendix A**

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

2. **Maximum Order** – 54151S / 132-51 \$500,000

3. **Minimum Order** - \$100

4. **Geographic Coverage** – 48 Contiguous States

5. **Point(s) of Production** – United States of America

6. **Discount from List Prices:** Prices shown are NET prices; Basic Discounts have been deducted.

7. **Quantity Discount** – Additional 0.5% on single task orders over \$250,000

8. **Prompt payment terms** – net 30 days

Credit Card Discount terms – None

9a. **Government Purchase cards accepted at or below micro purchase threshold** – Yes

9b. **Government Purchase cards accepted above micro purchase threshold** – Yes

10. **Foreign Items** – None



- 11a. **Time of delivery** – Negotiated at the task order level
- 11b. **Expedited delivery** – Negotiated at the task order level
- 11c. **Overnight and 2-day delivery** - Negotiated at the task order level
- 11d. **Urgent Requirements** - Negotiated at the task order level
- 12. **F.O.B. point(s)** – Destination
- 13a. **Ordering address(es)** – 3141 Fairview Park Dr., Suite 315, Falls Church, VA 22042
 - Ordering address:** Attention: Gary Kirkland
3141 Fairview Park Dr., Suite 315
Falls Church, VA 22042
Phone: (240) 493-7437
Email: contracts@agil3tech.com

 - Attention: Belinda Lowe
3141 Fairview Park Dr., Suite 315
Falls Church VA 22042
Phone: (703) 310-4286 or M: (301) 335-1323
Email: bd@agil3tech.com

 - Payment address:** Agil3 Technology Solutions
Attention: Accounts Receivables
3141 Fairview Park Dr., Suite 315
Falls Church, VA 22042
Ar_mail@agil3tech.com
- 13b. **Ordering procedures** – EDI Belinda Lowe, 3141 Fairview Park Dr., Suite 315, Falls Church, VA 22042
- 14. **Payment address(es)** – 3141 Fairview Park Dr., Suite 315, Falls Church, VA 22042
 - Warranty Provision – Standard Commercial Warranty
- 15. **Export Packing Charges** – None
- 16. **Terms and conditions of Government purchase card acceptance** – Accepted for above, at or below the micro purchase threshold.
- 17. **Terms and conditions of rental, maintenance, and repair** – None
- 18. **Terms and conditions of installation** – None
- 19. **Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices** – None
- 20a. **Terms and conditions for any other services** – See Section 3. Terms and Conditions
- 20. **List of service and distribution points** – None



21. **List of participating Dealers** – None
22. **Preventative maintenance** – None
- 24a. **Special attributes such as environmental attributes** – None
- 24b. **Section 508** – Not Applicable
23. **Data Universal Number System (DUNS) number** – 078681923
26. **Notification regarding registration in System for Award Management (SAM) database** – Active
Type of Contractor: Small Business
 - a. SBA Certified 8(a) Firm
 - b. SBA Certified Small Disadvantaged Business (SDB)
 - c. Women-Owned Small Business (WOSB)
 - d. Service-Disabled Veteran-Owned Small Business (SDVOSB)
 - e. Veteran-Owned Small Business (VOSB)
 - f. Economically-Disadvantaged Women Owned Small Business (EDWOSB)



Section 2. A3T Labor Category Rates and Descriptions

Appendix A: 54151S / 132-51 Labor Rates and Pricing

Agil3 Technology Solutions LLC Labor Rates

SIN	Service	Contract Year 6	Contract Year 7	Contract Year 8	Contract Year 9	Contract Year 10
54151S	Computer Forensic and Intrusion Analyst	\$117.85	\$120.21	\$122.61	\$125.07	\$127.57
54151S	Configuration Management, Journeyman	\$56.79	\$57.93	\$59.08	\$60.27	\$61.47
54151S	Cyber Security, Information Assurance Specialist, Entry	\$55.34	\$56.44	\$57.57	\$58.72	\$59.90
54151S	Cyber Security, Computer Security Specialist, Journeyman	\$63.14	\$64.40	\$65.69	\$67.00	\$68.34
54151S	Cyber Security Blue Team Specialist, Journeyman	\$63.14	\$64.40	\$65.69	\$67.00	\$68.34
54151S	Cyber Security Continuous Monitoring Specialist, Journeyman	\$63.14	\$64.40	\$65.69	\$67.00	\$68.34
54151S	Cyber Security Connection Approval Specialist, Senior	\$101.20	\$103.22	\$105.29	\$107.39	\$109.54
54151S	Cyber Security Info Assurance Policy Support Specialist, Journeyman	\$63.14	\$64.40	\$65.69	\$67.00	\$68.34
54151S	Cyber Security Info Assurance Vulnerability Management (IAVM) Specialist, Journeyman	\$63.14	\$64.40	\$65.69	\$67.00	\$68.34
54151S	Cyber Security, Network Defense Reporting Specialist, Journeyman	\$74.23	\$75.72	\$77.23	\$78.78	\$80.35
54151S	Cyber Security Ports, Protocols, and Services Management (PPSM) Specialist, Journeyman	\$69.80	\$71.19	\$72.61	\$74.07	\$75.55
54151S	Database Specialist, Senior	\$56.79	\$57.93	\$59.08	\$60.27	\$61.47
54151S	Functional Area Expert I	\$194.18	\$198.07	\$202.03	\$206.07	\$210.19
54151S	Help Desk Support Service Specialist, Intermediate	\$31.71	\$32.35	\$32.99	\$33.65	\$34.33
54151S	Managed Systems Engineer	\$53.26	\$54.33	\$55.41	\$56.52	\$57.65
54151S	Network Specialist Technician Intermediate	\$34.88	\$35.57	\$36.28	\$37.01	\$37.75



SIN	Service	Contract Year 6	Contract Year 7	Contract Year 8	Contract Year 9	Contract Year 10
54151S	Network Support Technician Senior	\$38.36	\$39.13	\$39.91	\$40.71	\$41.52
54151S	Subject Matter Expert I	\$166.44	\$169.77	\$173.17	\$176.63	\$180.16
54151S	Subject Matter Expert (Journeyman)	\$66.18	\$67.50	\$68.85	\$70.23	\$71.63
54151S	Subject Matter Expert (Senior)	\$135.95	\$138.67	\$141.44	\$144.27	\$147.16
54151S	Systems Administrator, Intermediate	\$48.72	\$49.70	\$50.69	\$51.71	\$52.74
54151S	Systems Engineer	\$58.93	\$60.11	\$61.31	\$62.54	\$63.79
54151S	Systems Engineer, Senior	\$77.12	\$78.66	\$80.23	\$81.84	\$83.48
54151S	Tier I, Technical Support II	\$37.65	\$38.40	\$39.17	\$39.95	\$40.75
54151S	Tier I, Technical Support III	\$42.37	\$43.21	\$44.08	\$44.96	\$45.86
54151S	Training Specialist, Journeyman	\$56.79	\$57.93	\$59.08	\$60.27	\$61.47
54151S	Consultant Expert	\$194.18	\$198.07	\$202.03	\$206.07	\$210.19
54151S	Application Engineer	\$93.94	\$95.82	\$97.74	\$99.70	\$101.69
54151S	Application Engineer, Senior	\$124.96	\$127.46	\$130.01	\$132.61	\$135.26
54151S	Configuration Manager	\$72.96	\$74.42	\$75.91	\$77.43	\$78.98
54151S	Counter-Intelligence Cyber Analyst	\$62.19	\$63.43	\$64.70	\$66.00	\$67.32
54151S	Cyber Security Engineer, Level I	\$135.49	\$138.20	\$140.97	\$143.79	\$146.66
54151S	Cyber Security Engineer, Level II	\$145.39	\$148.30	\$151.26	\$154.29	\$157.37
54151S	Cyber Security PKI Engineer	\$90.88	\$92.69	\$94.55	\$96.44	\$98.37
54151S	Cyber Security, Connection Approval, Lead	\$115.54	\$117.85	\$120.21	\$122.61	\$125.06
54151S	Cyber Security, Continuous Monitoring Specialist, Senior	\$103.13	\$105.20	\$107.30	\$109.45	\$111.63
54151S	Cyber Security, IA Development Engineer II	\$185.24	\$188.95	\$192.73	\$196.58	\$200.51
54151S	Cyber Security, IA Network Engineer	\$123.67	\$126.14	\$128.66	\$131.24	\$133.86
54151S	Cyber Security, IA Specialist, Journeyman	\$82.59	\$84.24	\$85.92	\$87.64	\$89.39
54151S	Cyber Security, IA Specialist, Senior	\$122.00	\$124.44	\$126.92	\$129.46	\$132.05
54151S	Cyber Security, Information Systems Security Officer (ISSO)	\$64.60	\$65.89	\$67.21	\$68.56	\$69.93
54151S	Cyber Threat Analyst	\$69.27	\$70.66	\$72.07	\$73.51	\$74.98
54151S	Cybersecurity Analyst	\$127.69	\$130.24	\$132.85	\$135.51	\$138.22
54151S	Database Administrator	\$82.29	\$84.35	\$86.03	\$87.75	\$89.51
54151S	Database Analyst/Programmer	\$78.87	80.45	\$82.06	\$83.70	\$85.37
54151S	Help Desk Specialist Senior	\$57.01	\$58.15	\$59.32	\$60.50	\$61.71



SIN	Service	Contract Year 6	Contract Year 7	Contract Year 8	Contract Year 9	Contract Year 10
54151S	Information Assurance Engineer	\$85.93	\$87.65	\$89.40	\$91.19	\$93.02
54151S	IT Cyber Security Project Manager	\$145.28	\$148.19	\$151.15	\$154.18	\$157.26
54151S	IT Operations Analyst	\$99.26	\$101.24	\$103.27	\$105.33	\$107.44
54151S	IT Program Analyst	\$120.88	\$123.30	\$125.77	\$128.28	\$130.85
54151S	IT Program Manager	\$135.63	\$138.34	\$141.11	\$143.93	\$146.81
54151S	IT Solutions Architect	\$143.54	\$146.41	\$149.34	\$152.32	\$155.37
54151S	IT Tech Support II	\$64.68	\$65.97	\$67.29	\$68.64	\$70.01
54151S	IT Tech Support III	\$67.06	\$68.40	\$69.77	\$71.16	\$72.59
54151S	IT Tech Support IV	\$74.14	\$75.62	\$77.14	\$78.68	\$80.28
54151S	Network Administrator	\$80.26	\$81.86	\$83.50	\$85.17	\$86.87
54151S	Network Engineer, Senior	\$124.96	\$127.46	\$130.01	\$132.61	\$135.26
54151S	Software Engineer	\$75.36	\$76.86	\$78.40	\$79.97	\$81.57
54151S	Software Engineer Intermediate	\$111.91	\$114.15	\$116.43	\$118.76	\$121.13
54151S	Systems Administrator Level I	\$68.11	\$69.47	\$70.86	\$72.27	\$73.72
54151S	Systems Engineer, Level I	\$92.35	\$94.19	\$96.08	\$98.00	\$99.96
54151S	Systems Engineer, Level II	\$98.48	\$100.45	\$102.45	\$104.50	\$106.59
54151S	Web Administrator	\$65.69	\$67.01	\$68.35	\$69.71	\$71.11
54151S	Web Software Developer	\$67.28	\$68.63	\$70.00	\$71.40	\$72.83



Appendix B: Labor Category Descriptions

Agil3 Technology Solutions LLC offers the following Labor Category Descriptions to support the effort contemplated herein.

Agil3 Technology Solutions, LLC (A3T) offers only the personnel who meet or exceed the minimum qualification requirements stated in the Labor Category Descriptions provided herein. *A3T* does allow experience to substitute for education requirements. Experience / Education substitutions applicable to all labor categories. *A3T*'s criterion for minimum experience substitution by educational degree is as follows.

High School	GED
Associates:	An Associate's degree may be substituted for one (1) year of experience when the minimum qualifications do not require a bachelor's degree.
Undergraduate:	An undergraduate degree may be substituted for 3 years of experience when the minimum qualifications do not require an undergraduate degree. Four (4) years of related experience may be substituted for an undergraduate degree.
Graduate or Above:	A graduate and/or higher degree may be substituted for three (3) years of experience when the minimum qualifications do not require a graduate or higher degree.

GSA and/or the ordering activities may have access to any *A3T* employee resume (by request) before, during or after assignment of any GSA order. If for some extenuating reason a person assigned to an order must be replaced or substituted, the ordering activity will be notified in advance, in writing, and the substituting personnel will have equal or greater qualifications than the departing employee.

Commercial Job Title/Labor Category	Responsibility, Experience, and Education
Application Engineer	<p>Functional Responsibility: Provides administration and maintenance of enterprise document management systems and applications in compliance with the organization's policy and guidance of documents. This includes maintaining both internal and external web sites which remain coherent and accessible and follow industry best practices as well as complying with applicable Federal requirements. Applies web design skills to maintain both the internal and external web sites. In addition, works with technical staff, gathering business requirements, developing process flows, creating and completing documentation, creating project time lines, and communicating project status. Responsibilities may also include end-user documentation, end-user training or train-the-trainer, and testing.</p> <p>Minimum/General Experience: Three (3) years of general IT / IS experience</p>



Application Engineer, Senior

Minimum Education: Bachelor's Degree or equivalent or six (6) years of related experience.

Functional Responsibility: Provides administration and maintenance of enterprise document management systems and applications in compliance with the organization's policy and guidance of documents. This includes maintaining both internal and external web sites which remain coherent and accessible and follow industry best practices as well as complying with applicable Federal requirements. Applies web design skills to maintain both the internal and external web sites. In addition, works with technical staff, gathering business requirements, developing process flows, creating and completing documentation, creating project timelines, and communicating project status. Responsibilities may also include end-user documentation, end-user training or train-the-trainer, and testing.

Minimum/General Experience: Five (5) years of general IT / IS experience

Computer Forensic and Intrusion Analyst

Minimum Education: Bachelor's degree or equivalent or seven (7) years of related experience.

Functional Responsibility: Provides knowledge in computer and network forensics, Identify, collect, examine, analyze, and preserve integrity of resources and information for computer forensics. Conducts vulnerability assessments/penetration tests of information systems. Develops, researches and maintains proficiency in tools, techniques, countermeasures, and in trend 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. Perform root cause analysis of computer systems that failed or are not operating properly when tasked by management. Incorporate approved forensic tools and develop standard processes for conducting forensics to ensure that incident handlers and first responders satisfy forensics and evidence requirements. Provide detailed reports written in plain business language on what happened, when it happened, how it happened, and who was involved after completion of the investigation. Conduct forensics work in such a manner that the information remains forensically sound and a strict chain of custody is maintained on the data.

Minimum/General Experience: A minimum of six (6) years professional experience. Professionally certified, within a CND disciplines are a plus.

Minimum Education: Requires a bachelor's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Configuration Management, Journeyman

Functional Responsibility: Provides configuration management planning, describes provisions for configuration identification, change control, configuration status accounting and configuration audits; Regulates the change process so that only approved and validated changes are incorporated into product documents and related software.

Minimum/General Experience: A minimum of four (4) years professional experience. Professionally certifications are a plus.

Minimum Education: Requires a bachelor's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Configuration Manager

Functional Responsibility: Performs configuration management (CM) of developmental and operational systems. Works on developmental and operational teams to create and maintain configuration baselines, including development, test, and production that supports developmental and operational systems. Uses and/or recommend automated CM tools to implement CM policies and procedures. Develops or modifies CM plans, policies, and procedures tailored to the complexity and scope of the developmental or operational system. Implements CM for the entire life cycle of systems from initial requirements or capabilities baselines to system end-of-life. Performs change control and configuration audits. Knowledge of hardware and software configuration management concepts, goals, benefits and standard strategies to achieve those goals, leading the communications campaign to promote awareness and acceptance of the CM program, and develops and conducts individual and group CM training workshops and seminars accordingly. Knowledge of developing, distributing, and tracking all change request packages resulting from Configuration Control Board actions. Skill maintaining a master library of both mission and support software, including Critical Success Factors (CSFs) and Key Performance Indicators (KPIs),



maintaining current inventories of all network and systems-related hardware, and developing reports to satisfy downward-directed data calls, audits, warranty and other maintenance support contracts/agreements, lifecycle management and budget projections.

Minimum/General Experience: Five (5) years of general IT / IS experience

Consultant Expert

Minimum Education: Bachelor's Degree or equivalent or seven (7) years related IT experience. With a Master's Degree, three (3) years of general experience is acceptable.

Functional Responsibility: Develops and applies advanced methods, theories, and research techniques in investigating and solving complex concept, planning, design, or implementation problems. Recognized for achievements and technical subject expertise.

Minimum/General Experience: Must have eight (8) years of Expertise in the respective field of services performed. At least four (4) of those years must be directly related to the required area of expertise.

**Counter-Intelligence
Cyber Analyst**

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities. Recognized for industry or subject achievements and technical expertise

Functional Responsibility: Support the counterintelligence (CI) mission by providing CI Cyber input into CI missions. Provides all-source CI cyber analysis with a focus on Advanced Cyber Threats. Provides cyber threat and intelligence analysis and develops briefings and reports to distribute and aid in information sharing and protection efforts. Assist with CI investigations by providing CI Cyber input to Risk Assessments, Damage Assessments, and Threat Assessments subsequent to Cyber-attacks and vulnerabilities. Provides classified cyber threat and intelligence briefings to senior government officials and prepares classified and unclassified reports for sharing with other agencies and working groups. Maintains subject matter expertise on existing and emerging cyber threats and threat actors.

Minimum/General Experience: Six (6) years counterintelligence (CI) experience through military or government agency; 1-year experience conducting CI Source operations.

**Cybersecurity
Analyst**

Minimum Education: Graduate of DoD/Federal Counterintelligence/Law Enforcement Badge & Credentialing School.

Functional Responsibility: Performs analysis of systems, programs and/or planning activities. Duties include the development of policies, procedures, and other technical documentation and the analysis of IA/Cyber related programs and initiatives. Duties may also include the design, development, and coordination of relationships and solutions to resolve problems within the specialty area. The position requires substantial knowledge of advanced theory and current practices in cybersecurity utilizing analytical skills.

Minimum/General Experience: 8 years of experience in Information Assurance or Cybersecurity.

**Cyber Security,
Continuous
Monitoring
Specialist, Senior**

Minimum Education: Bachelor's degree, one year of experience can be substituted by 15 semester hours completed towards a Master's degree in a related field. Two years of experience can be substituted by completion of a Master's degree in a related field.

Functional Responsibility: support the customer at the tactical level in the monitoring attempted intrusion, as well as performing security assessments on IT assets. The position will support the onsite Cyber/IA Security Lead implementing and improving technology and procedures related to vulnerability management, device hardening, and cyber security incident response. The Information Assurance Assessor will perform continuous monitoring of the enterprise infrastructure. The Information Assurance Assessor will prepare materials used to meet with and educate other information technology teams and business partners on security incidents, and vulnerability remediation guidance related to on demand, regular vulnerability scans, and penetration testing results.

Provides tactical Continuous Monitoring (ConMon) maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Provides



detailed evaluation and internal control and audit reviews of computer information systems; Perform Network vulnerabilities research and investigations, including proposal of alternative design options. Investigates (researches) available tools and countermeasures to remedy detected network vulnerabilities and recommends solutions and best practices; Analyzes and assesses vulnerabilities in infrastructure (software, hardware, networks); Monitors various alerts from alarms within the Cyber Security IT Infrastructure; Monitors data from various sources including intrusion detection systems and other security infrastructure components and firewalls.

Minimum/General Experience: 3-4 years' related experience in Information Assurance and IT Security in a Federal Government Agency; Must hold CompTia Security+ w/CE certification (equivalent or higher)

Minimum Education: Equivalent Bachelor's Degree in related discipline or the equivalent (combination of education, Cyber security technical certifications or training, or work experience).

Cyber Security,
Connection Approval
Lead

Functional Responsibility: Functional responsibilities include leading the Connection Approval Packages (CAP) Team; reviewing and determining if system/application documentation is accurate, up to date, and displays thorough details that provide a clear security posture of the system/application being assessed. Maintains a repository of all documentation collected for all Assess Only packages to include decommissioned systems/applications. Stays in contact with the customer throughout the assessment and authorization of the Assess Only/CAP process/procedures and follow the escalation process until authorization, disconnection, or decommission is achieved. Assembles all documentation established by organization guidelines and supporting materials for review to the Government for approval. Considers recommendations and or directions communicated during the approval process to correct deficiencies in documentation or to eliminate vulnerabilities. Provides recommendations on how to efficiently develop methods, procedures, technical requirements regarding assess only or CAP procedures. Proficient with RMF process, NIST SP 800-37, NIST SP 800-53, CNSSI 1253. Demonstrate leadership skills and has customer service experience/skills.

Minimum/General Experience: 5+ years of experience in RMF certification (CASP or CISM)

Minimum Education: Bachelor's degree

Cyber Security
Engineer, Level I

Functional Responsibility: Directs and performs information systems engineering analysis for testing, assessing, evaluating, integrating, and enforcing requirements of Cybersecurity/IA products and tools to coordinate assessment and acquisition. Duties include assessment and evaluation of system architectures, vendor descriptions and technical application guides; interfacing with testing laboratories; and reviewing solutions to ensure compliance with existing and emerging policies.

Minimum/General Experience: Minimum eight (8) years of experience in Information Assurance or Cybersecurity.

Minimum Education: Bachelor's degree, one year of experience can be substituted by 15 semester hours completed towards a Master's degree in a related field. Two years of experience can be substituted by completion of a Master's degree in a related field.

Cyber Security
Engineer, Level II

Functional Responsibility: Under general supervision, provide a full range of cyber security and endpoint (e.g. HBSS) administrative functions to ensure compliance with instructions, regulations, memorandums and procedures from higher echelons. Analyze trends, develop solutions, present findings and make technical decisions in support of endpoint optimization. Duties include: Installation and upgrade of agent client modules; Installation and upgrade of point product modules; Development and maintains of policies for point product modules; and Maintain compliance with mandates locally and non-locally. Maintain backup copies of all policies; Maintenance of endpoint configuration; Remediation of local server operating system findings, software findings, and SQL server findings identified via vulnerability scans; Recommend and implement organizational process improvements to promote efficiency of overall end-point security system operations. Performs endpoint vulnerabilities research and investigations, including proposal of alternative solutions to



mitigate risks; Investigates (researches) available tools and countermeasures to remedy detected vulnerabilities, and recommends solutions and best practices; Analyzes security event audit log information from network security devices (e.g., network and host-based security systems, firewalls, routers, switches, etc.) and mission critical servers for anomalies and known attack patterns, etc.

Minimum/General Experience: 5+ year' experience

Minimum Education: CompTIA Security Plus CE; User and Admin modules certifications (as applicable)

Functional Responsibility: Under general guidance, provide Information Assurance (IA)/Computer Network Defense Support, using enterprise-level integrated software solutions that provides automated network vulnerability scanning, configuration assessment, and network discovery, IA Oversight and compliance, Assessment and Authorization (A&A) Development, and IA Program Support. Provide assessments of threats and vulnerabilities, determining deviations from acceptable configurations, assessing the level of risk and developing and/or recommending appropriate mitigation / countermeasures in the operational environment. Perform vulnerability scanning and provide technical support for the enterprise-level integrated software solution to ensure confidentiality, integrity and availability of the network. Provide security scanning and IA technical support to customer organizations. Coordinate with external entities to perform required compliance reporting. Report IA compliance posture to IA management, command, and stakeholders in accordance with IA internal and external reporting requirements. Assist with the development, coordination and maintenance of A&A packages in accordance with the Risk Management Framework (RMF) Process.

Cyber Security, IA
Development
Engineer II

Minimum/General Experience: Eight (8) years of direct experience in IA/CND/CyberSecurity

Minimum Education: Bachelor's Degree or higher in a related technical discipline, or the equivalent (combination of education, Cyber security technical certifications or training, or work experience).

Functional Responsibility: Under general guidance, conduct assessment of information systems security controls to include technical controls. Conduct risk and security control assessments and risk analysis and drafting Security Assessment Reports and recommendations for system's non-compliant security controls IAW NIST 800-30; and DoD/customer processes. Document results and submit recommendations to SCA. Conduct Continuous Monitoring activities such as Annual Assessment evaluations and Analyze system's POA&Ms, providing recommended mitigations and needed fix timelines. Review proposed mitigations, requests for risk acceptance, and the rationale provided for stated residual risk acceptance. Provide evaluation results on an official form used to verify awareness of or risk acceptance by leadership. Analyze proposed system changes, determining minor or significant change and provide guidance on appropriate technical security testing. Complete accurate documentation in all Microsoft product formats and effectively brief agency management, Security Control Assessors (SCA) and Authorizing Official (AO) as required.

Cyber Security, IA
Network Engineer

Minimum/General Experience: 7 years of experience in IA Policy / cybersecurity

Minimum Education: Bachelor's Degree or higher in a related technical discipline, or the equivalent (combination of education, Cyber security technical certifications or training, or work experience).

Functional Responsibility: Works on IA teams involving all phase of information assurance; implements information assurance/security standards and procedures, 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 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, ensures that all information systems are functional and secure.

Cyber Security,
Information
Assurance
Specialist, Entry

Minimum/General Experience: A minimum of two (2) years professional experience. Professionally certified, within an IAM or CND discipline is a plus.



Cyber Security, IA
Specialist
Journeyman

Minimum Education: Requires an associate's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Functional Responsibility: Provides Information Assurance (IA), technical support, and Cyber Security industry best practices to assure the security posture of the organization. Supports the development and implementation of information assurance/security policies; coordinates, develops, and evaluates the security posture for the organization. This includes analyzing and defining security requirements for computer systems (i.e. servers, workstations, laptops, mobile devices, etc.), and satisfying information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Recommends information assurance and security solutions to support customers' requirements. IAW FISMA/NIST/Federal/customer requirements, performs analysis, design, and development of security features for system architectures, and implements solutions that meet security requirements; Assists with implementation and maintenance of security technologies and components; Investigates general information assurance-related technical problems and provides basic technical support in solving these problems; Prepares for and manages inspections, audits, governance initiatives and assessments as part of an integrated program; Develops risk management guidelines and recommend improvements to accreditation processes; Monitors applicable Federal and commercial security alerts and providing updates and advice to federal IT staff regarding protective measures to avoid breaches.

Minimum/General Experience: 3 years related experience in Information Assurance and IT Security in a Federal Government Agency; Must hold CompTia Security+ w/CE certification or industry equivalent

Cyber Security, IA
Specialist Senior

Minimum Education: Associates Degree (IT, Engineering, Cybersecurity, etc.) or 2 more years' technical experience.

Functional Responsibility: Provides Information Assurance (IA), technical support, and Cyber Security industry best practices to assure the security posture of the organization. Support the development and implementation of information assurance/security policies; coordinates, develops, and evaluates the security posture for the organization. This includes analyzing and defining security requirements for computer systems (i.e. servers, workstations, laptops, mobile devices, etc.), and satisfying information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Recommends information assurance and security solutions to support customers' requirements. IAW FISMA/NIST/Federal/customer requirements, performs analysis, design, and development of security features for system architectures, and implements solutions that meet security requirements; Assists with implementation and maintenance of security technologies and components; Investigates general information assurance-related technical problems and provides basic technical support in solving these problems; Prepares for and manage inspections, audits, governance initiatives and assessments as part of an integrated program; Develop risk management guidelines and recommend improvements to accreditation processes; Monitors applicable Federal and commercial security alerts and providing updates and advice to federal IT staff regarding protective measures to avoid breaches.

Minimum/General Experience: 5 years in IT Security and Certification and Accreditation for a Federal Government Agency; Must hold one of the following certifications: CISSP, CASP, CISM, or CISA or industry equivalent

Minimum Education: Bachelor's Degree (IT, Engineering, Cybersecurity, etc.) or an additional 3 years' technical experience.

Functional Responsibility: The Computer Security Specialist will perform studies, tests, and evaluations of security devices and systems. Will develop documentation and will conduct interviews with technical personnel incidental to and as required to perform security risk assessments. Will perform assessments in order to determine the level of computer and network security necessary to implement proposed information systems. Applies knowledge of current IA policy, tactics, techniques, policy, and doctrine, and relationship to IA reporting requirements and structure.

Cyber Security,
Computer Security
Specialist,
Journeyman



Cyber Security Blue
Team Specialist,
Journeyman

Minimum/General Experience: A minimum of six (6) years professional experience. Professionally certified, within a CND discipline is a plus.

Minimum Education: Requires an associate's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Functional Responsibility: Perform Security Assessment Program technical and non-technical Independent Verification & Validation (IV&V) assessment missions for any customer security missions, programs, plans, and security requirements affecting the confidentiality, integrity, availability, non-repudiation and accountability of an effective and hardened security posture. Conduct in-depth Vulnerability Assessments and Information System Auditing of assets (e.g., servers, Workstations, Network Appliances, Storage Devices, and Applications). Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle, ensures that all information systems are functional and secure. Use automated and manual testing, examination, scanning, interviewing, and discovery techniques to identify, validate, and assess security vulnerabilities and mitigate vulnerabilities to strengthen computer security posture against cyber aggressors. Validate, and assess vulnerabilities, to report whether or not specific security objectives and goals are being met and where applicable, compliance IAW FISMA, DODI 5200.40, 8500.2 and NIST SP 800-115 and industry best practices. This includes but not limited to Server & Workstation Devices (Windows, Unix, & Linux), Network Devices (Routers, Switches, Video Teleconference), Storage Devices (Fibre Channel Switches, Network Attached Storage, Storage Controllers) Applications (Web, Database, Email, FTP, SSH), Security Devices (Firewalls, Intrusion Detection Systems, Web Content Filters).

Minimum/General Experience: A minimum of two (2) to six (6) years related professional experience. Professionally certified, within a CND discipline is a plus.

Knowledge of interrelation of different safeguards and how they impact the overall protection of an environment is crucial. Must have the ability to support technical analysis document and present reports to the supported organization.

Minimum Education: Requires an associate's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Cyber Security
Continuous
Monitoring
Specialist,
Journeyman

Functional Responsibility: Support the strategic and tactical Continuous Monitoring (ConMon) Program evaluating technology, processes, procedures, operating environment, and people. Continuous Monitoring is defined by NIST as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Utilize DOD, DHS, NIST, FISMA, and other government standards, policy, regulations, etc. (NIST 800-137, NIST 800-53, 800-37 and 800-39) to execute on the ConMon Program. Analyzes general ConMon information assurance-related tools and processes and provides ongoing awareness and insight of the organizations security posture. Gathers relevant and up-to-date (near real-time) information about risk, threats, vulnerabilities, system and enterprise controls.

Minimum/General Experience: A minimum of four (4) years related professional experience. Professionally certified, within a CND discipline is a plus.

Knowledge of interrelation of different safeguards and how they impact the overall protection of an environment is crucial.

Minimum Education: Requires an associate's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Cyber Security
Connection Approval
Specialist, Senior

Functional Responsibility: Administer the Connection Approval Program and Tenant Security Process in accordance with organization's regulation or policy to support tenant organizations as well. Providing these tenant organizations with CAP support throughout the life cycle of their system. Support all activities needed to obtain certification and accreditation on all the networks, equipment and systems at all classification levels. Ensure required CAP documentation is obtained from all current and new customers. Review all packages received for completeness and accuracy and maintain CAP Packets. Maintain CAP documentation for each connection to the backbones. Ensure that packages are updated when there are modifications, additions or changes to tenant networks. Administer the Tenant Security Plan (TSP) Process for all tenants that connect to the network(s) and provide Tenant Security Plans for review and signature. Support Customer efforts to certify and accredit standalone equipment. Maintain a complete and accurate identification of all



information systems that connect to the network(s). Support and assist in coordination of Agent of the Certification Authority (ACA) visits and provide ACA Audit Reports.

Minimum/General Experience: A minimum of three (3) or more years of IT Security and Connection Approval related professional experience. Professionally certified, within an IAM discipline is a plus.

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities.

Cyber Security Info Assurance Policy Support Specialist, Journeyman

Functional Responsibility: Validate User Authorization Request (UAR) using the ticketing program (Remedy) to process and monitor progress of all Privileged level and User account requests for JWICS, SIPR and NIPR. Within the Information Assurance Project Management (IAPM) team, ensure the account requests are accurate, complete and have the following documents: Privileged Level Access Agreements, Appointment Orders, DD 2875s, training and certification documentation, up to date annual awareness training, and most recent version of agency's Acceptable Use Policy. Utilize the Training Certification Tracking system to verify user account request information. Process the documents for government signature. Draft, coordinate, and track Acceptance of Risk documents (AORs), Exception to Policy (ETP), in accordance with AR 25-50, and local SOPs, and to maintain an Automated Dashboard for tracking. Ensure all pertinent documents are included in the package for DAA review and signature.

Minimum/General Experience: Four (4) years of related experience. Professionally certified, within an IAM discipline is a plus.

Minimum Education: An associate's degree from an accredited university or college preferred or a combination of education and experience that provides the required knowledge, skills, and abilities.

Cyber Security Info Assurance Vulnerability Management (IAVM) Specialist, Journeyman

Functional Responsibility: Supports all aspects of vulnerability management to include identifying and acknowledging IAVM notices; reviewing, tracking, and verifying IAVM compliance; conducting vulnerability scans; and performing vulnerability trend analysis and metric reporting. Support vulnerability management program in accordance with the CJCSM 6510.01. Identify, respond to, and perform work activities associated with all IAVM notices issued. Conduct vulnerability assessments on assets and review results to verify targeted assets (e.g. servers, workstations, laptops, printers, and network appliances (routers, switches, firewalls, intrusion detection systems, etc.) conform to security requirements and submit results to stakeholders. Review Plan of Action & Milestones (POA&Ms) for completeness, verify applicable timelines are on track to be met, and work with system owners to rectify discrepancies. Scanning tools may include Q-Tip, ACAS, and Retina. Develop and maintain an IAVM tracking system to facilitate performing trend analyses, generate IAVM reports, and tracking metrics for executive level leadership. Investigate false positive scan results. If confirmed, notify appropriate stakeholders to report finding and provide evidence. Support and provide technical expertise for Change Management process.

Minimum/General Experience: Four (4) years of related experience. Network scanning experience – Retina and ACAS training, and a professional certification, within a CND discipline is a plus.

Knowledge of interrelation of different safeguards and how they impact the overall protection of an environment is crucial.

Minimum Education: Requires an associate's degree from an accredited university or college or a combination of education and experience that provides the required knowledge, skills, and abilities.

Cyber Security, Information Systems Security Officer (ISSO)

Functional Responsibility: Responsible for Information System Security Officer (ISSO) End User Support to organization components and on-boarded organizations; maintaining awareness of current cybersecurity developments and issues; and supporting the accreditation of systems and applications. Initiates the Risk Management Framework (RMF) accreditation of new systems, and the reaccredits expired/expiring systems; and coordinates with other teams to create and distribute CS policy, processes, and guidance to supported organizations and components.

Minimum/General Experience: 2 years in a relevant field

Minimum Education: Bachelor's Degree or 4 additional years' experience in a relevant field.

Functional Responsibility: Draft CND alerts, warnings, orders, notifications and other products for CND Community customers. Proven experience and ability to leverage CND analyst toolsets to detect

Cyber Security, Network Defense



**Reporting Specialist,
Journeyman**

and respond to IT security incidents. Conducts research and document threats and their behavior to include monitoring external CSIRTS/CERTs. Assist in providing recommendations to threat mitigation strategies. Employ effective web, email, and telephonic communications to clearly manage security incident response procedures. Consolidates trending of cyber incidents and creates the products that are required to be used for briefing leadership, partners, and customers regarding computer network defense. Experience required in security or network technology (Unix/Windows OS, Cisco/Juniper Routing-Switching) within a hands-on Implementation or Administration role. Demonstrates thorough knowledge of TCP-IP protocol implementations for all common network services in addition to demonstrated capability to perform network packet analysis and anomaly detection.

Minimum/General Experience: Four (4) years+ of experience performing duties similar to those described above; Strong written and oral communications skills. Professionally certified, within a CND discipline is a plus.

Minimum Education: Requires a bachelor's degree in an associated discipline or a combination of education and experience that provides the required knowledge, skills, and abilities.

**Cyber Security Ports,
Protocols, and
Services
Management (PPSM)
Specialist,
Journeyman**

Functional Responsibility: Determines enterprise information assurance and security standards. Supports Ports, Protocols, and Services Management (PPSM) and the DOD DMZ Whitelist program, which provides implementation guidance on the use of IP protocols, application, systems and data services that traverse the DOD Networks and supports net centric operations. Ensure Enterprise Information System Ports, Protocols, and Services are registered in the PPSM central registry and not deployed prior to DAA approval; develop, revise, implement, and enforce PPSM policies. Conduct PPSM reviews and generate an Exception Request Summary that identifies PPS, enclaves and boundaries of traffic, required customer coordination, status of the request and recommends risk mitigations. Coordinate and submit Non-Standard Use (NSU) packages to the Defense Information Assurance Security Accreditation Working Group (DSAWG) for action. Submit approved white list exceptions to the DOD DMZ Whitelist. Collect and aggregate PPSM & Whitelist artifacts, trends, and performance metrics.

Minimum/General Experience: A minimum of two (2) years+ experience performing duties similar to those described above. Professionally certified, within a CND discipline is a plus.

Minimum Education: Associates Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities.

**Cyber Security PKI
Engineer**

Functional Responsibility: Research, analyze, and develop recommendations for PKI requirements and future technology advancements. Must possess strong understanding of current cybersecurity posture and future requirements. Must possess understanding of cybersecurity policy, procedures, processes, and associated documentation. Evaluate and provide AoA for emerging technologies. Develop white papers on technological developments. Must have strong written and oral communication skills with basic database understanding. Minimum eight years of experience in Cybersecurity or PKI. Must have a Bachelor's degree and a DoD 8570.1M IAM-II certificate, one year of experience can be substituted by 15 semester hours completed towards a Master's degree in a related field. Two years of experience can be substituted by completion of a Master's degree in a related field.

Minimum/General Experience: Eight (8) years of experience in Cybersecurity or PKI.

Minimum Education: Bachelor's degree and a DoD 8570.1M IAM-II certificate, one year of experience can be substituted by 15 semester hours completed towards a Master's degree in a related field. Two years of experience can be substituted by completion of a Master's degree in a related field.

Cyber Threat Analyst

Functional Responsibility: Conducts complex, all-source computer network operations (CNO)/Computer Network Defense (CND)-related intelligence analyses; prepare and coordinate high-level Cyber Threat intelligence assessments. Provides cyber threat and intelligence analysis and develops briefings and reports to distribute and aid in information sharing and protection efforts. Provide information concerning adversary cyber actions and capabilities to the Government. Use all-source analysis and all available intelligence disciplines to research, draft, and submit information to the Government.

Minimum/General Experience: 6 years of experience as an All Source intelligence analyst



supporting Cyber activities or preparing finished intelligence products and briefing and operations for a United States Government organization

Database Administrator

Minimum Education: Bachelor's degree

Functional Responsibility: Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data. Performs all administrative functions in support of the database including: controlling access to the database; ensuring the safekeeping of the data; monitoring the use; develop standards, procedures, and conventions for use; performing system application and software installation, testing, recovery and reorganization, and configuration management and deployment of application software; maintaining a system trouble log; and training operators in the use of the database. Demonstrates knowledge and experience in all functions of database administration. Hands-on experience in application programming and design using a relational database management application.

Minimum/General Experience: 4 years' experience

Database Analyst/Programmer

Minimum Education: Bachelor's Degree or seven years of IT. With a Master's Degree, three (3) years of IT experience is acceptable.

Functional Responsibility: Designs, implements and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, and integration of systems through database design. Competent to work at the highest level of all phases of database management.

Minimum/General Experience: 4 years' experience

Database Specialist, Senior

Minimum Education: Bachelor's with 3 more years' experience

Functional Responsibility: Provides all activities related to the administration of computerized databases. Projects long-range requirements for database administration and design in conjunction with other managers in the information systems function. Designs, creates, and maintains databases in a client/server environment. Conducts quality control and auditing of databases in a client/server environment to ensure accurate and appropriate use of data. Advises users on access to various client/server databases. Designs, implements, and maintains complex databases with respect to JCL, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, and statistical methods. Applies knowledge and experience with database technologies, development methodologies, and front-end (e.g., COGNOS)/back-end programming languages (e.g., SQL). Performs database programming and supports systems design. Includes maintenance of database dictionaries, overall monitoring of standards and procedures, file design and storage, and integration of systems through database design.

Minimum/General Experience: A minimum of five (5) years of experience performing duties similar to those described above.

Minimum Education: Bachelor's Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities.

Functional Area Expert I

Functional Responsibility: Serves as the subject-matter expert (SME) who analyzes user needs to determine functional requirements that apply to automatic data processing (ADP) equipment or solutions. Works with engineers and technical analysts to incorporate functional requirements into new or existing systems. May remain involved through system design and implementation.

Minimum/General Experience: Fifteen (15) years of experience and recognized as a functional expert on the subject

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities.

Help Desk Specialist Senior

Functional Responsibility: Under general supervision, Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments.



May supervise others.

Minimum/General Experience: 5 years' experience

Help Desk Support
Service Specialist,
Intermediate

Minimum Education: High School Diploma

Functional Responsibility: Under general supervision, provides second-tier support to end-users for PC, server, mainframe applications and hardware. Handles problems that the first-tier of help desk support is unable to resolve. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Maintains currency and high level of technical skill in field of expertise. Escalates more complex problems to Senior Level.

Minimum/General Experience: A minimum of three (3) years of related experience in a networked environment.

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities.

Information
Assurance Engineer

Functional Responsibility: Responsible for all activities relating to information assurance procedures and systems. Develops information systems assurance programs and control guidelines. Confers with and advises subordinates on administrative policies and procedures and resolving technical problems, priorities, and methods. Consults with and advises other sections regarding internal controls and security procedures. Prepares activity and progress reports relating to the information systems audit function.

Minimum/General Experience: 6 years' of IT experience with 2 years in the Information Assurance area

Minimum Education: BS degree in Engineering, Math, Computer Science or 5 years additional Information assurance experience

IT Cyber Security
Project Manager

Functional Responsibility: Provides expert level planning, coordinating, scheduling, resourcing, tracking, documenting, executing, applying compliance standards and analyzing audits and inspections delivering large/complex projects on time within budget within an organization. Provide support for cyber security-related audits, inspections and assessments, including managing projects, serving as trusted agent, conducting site/staff assistance visits (SAV), command cyber readiness inspections (CCRI), and manual compliance assessments, and ensuring compliance with Cyber Security Service Provider (CSSP) evaluation criteria.

Supports the Audit and Inspection Project Management program, including but not limited to assisting the government in planning, coordinating, scheduling, resourcing, tracking, documenting, executing, and improving audits and inspections performed by external organizations upon the enterprise, as well as self-audits, self-inspections and Subscriber audits/inspections performed by organization. Supports the Trusted Agent Program, including but not limited to assisting the government in coordinating, de-conflicting, communicating, and facilitating between internal and external organizations to prevent potential interruptions to internal networks, systems and services. Evaluate the design and effectiveness of controls and standards to ensure cybersecurity compliancy in accordance with the applicable audits and inspections for an organization. Demonstrated expert level understanding of vulnerabilities/weaknesses across complex IT environments and ability to understand applicability of security standards across technologies.

Minimum/General Experience: 6 years IT program/project management experience with 3 years IT program management experience supporting the Federal Government.

Minimum Education: BS in a Business or IT focus or 4 additional years' experience or a DoD 8570 IAM Level III certification or Industry equivalent

IT Operations
Analyst

Functional Responsibility: Develops and applies advanced methods, theories, and research techniques in investigating and solving complex concept, planning, design, or implementation problems to support Operations mission. Analyzes existing and potential product and service information and prospective customers and markets. Provide expert level support, research,



analytical, technical, functional, administrative, and management support in the development of information for presentation, documentation and collaboration in support of mission. Employs multiple research techniques and interview procedures to gain the needed information to deliver Information Papers, White papers, instructional aids, exhibits for production, etc. Collates information into meaningful products, reports and presentation material. Maintains any technical information in a systems library.

Minimum/General Experience: 3- years' experience

Minimum Education: Bachelor of Science in a Technically related field or 4 years additional experience

IT Program Analyst

Functional Responsibility: Coordinates with key stakeholders to identify and document long-term strategic plans and assist in the development of resource requirements to support IT Governance & Enterprise Initiatives. Plans and conducts analyses of management, organizational and business improvement services and conceptualizes and defines the problems. Assists in the development of alternatives and solutions to a variety of problems; analyzing requirements; system documentation, and operational conditions to determine how to meet business and mission needs. Provides IT Program Analytics and Strategic Planning support to the CIO, including but not limited to Critical IT governance functions that ensure integrity through continuous management of IT resources, availability, and uptime. Plans, organize, and carry through to completion analytical studies to achieve effective, efficient, productive, and substantive enterprise-level programs. Prepares local directives, memoranda, policy statements, proposals, and other written documents to include web content in support of Government initiatives. Assesses costs benefits, evaluate feasibility, and develop options for courses of actions identifying the recommended course of action in support of current and future programs. Analyzes program functions and/or areas to discern trends in program delivery. Participates in mission related meetings and briefings and advises the Government of any problems or potential problems affecting performance.

Minimum/General Experience: 4 years professional experience within Federal Government imperatives/policies disciplines

Minimum Education: Bachelor's Degree in a Business or IT-related discipline

IT Program Manager

Functional Responsibility: Responsible for the overall management of the specific task order(s) and ensuring that the program's technical solutions and schedules are implemented in a timely manner. Performs enterprise wide horizontal integration planning and interfaces to other functional systems. Provides for the planning, monitoring, analyzing, executing and close out of various technical support projects assigned to Help Desk, Data Center, and other contractor staff. This includes providing project personnel with guidance on all areas of the engagement and performing as the primary customer contact for all IT support issues throughout the duration of the program. Assists IT management in defining the project scope, deliverables, and requirements for projects; Define priorities and establish project standards to ensure integrity and quality of project deliverables; Planning project activities, tasks, milestones, resources, and performance measures ensuring contractor staff comply with IT technical requirements and quality assurance.

Minimum/General Experience: 6 years IT experience with 3 years of supervisory-related experience

Minimum Education: Bachelor's Degree in Business or IT or a Bachelor's degree in a non IT Field coupled with 8 years total experience.

IT Solutions Architect

Functional Responsibility: Understands Client's Business Environment, Enterprise IT Management Processes. Develops detailed Design/Blueprints for IT Products. Defines reusable components/frameworks, common schemas, standards and tools. Provides domain expertise and guidance as to the (business and Technical) requirements. Maps requirement, Solutions outline, use case development and high-level design. Develops and delivers research, whitepapers, concepts, and processes. Executes Proof of Concepts as needed. Develops Detailed Design of Workflows, Custom adapters and interfaces utilizing APIs etc. Developing detailed custom solutions based on Client requirements. Actively participates in decision making with Client Teams and seek



to understand the broader impact of decisions.

Minimum/General Experience: 8 years IT experience

IT Tech Support II

Minimum Education: Bachelor's Degree in Computer Science or Related Discipline or 4 years IT experience

Functional Responsibility: Under general supervision, provides daily local help desk support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed under this contract or predecessors. Serves as the initial point of contact for troubleshooting hardware/software PC and printer problems. Maintains and updates service ticket tracking tool.

Minimum/General Experience: 2 years general IT/IS experience

IT Tech Support III

Minimum Education: High School diploma or equivalent

Functional Responsibility: Under general supervision, provides daily local help desk support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed under this contract or predecessors. Serves as the initial point of contact for troubleshooting hardware/software PC and printer problems. Maintains and updates service ticket tracking tool.

Minimum/General Experience: 4 years general IT/IS experience

IT Tech Support IV

Minimum Education: High School diploma or equivalent

Functional Responsibility: Provides daily local help desk support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed under this contract or predecessors. Serves as the initial point of contact for troubleshooting hardware/software PC and printer problems. Maintains and updates service ticket tracking tool. May serve as the team lead and/or supervisor for more junior team members staffing the help desk.

Minimum/General Experience: 6 years applicable experience

Managed Systems Engineer

Minimum Education: High School diploma or equivalent

Functional Responsibility: Under general direction, performs duties such as site surveys, architecture design, system evaluation, system analysis, and infrastructure assessment. The managed system engineer shall perform duties on tasks that require expertise in system/processor architecture, wired for management baseline, desktop management interface, SNMP, client/server architecture, operating systems, software applications, network protocols, routers, switches, remote access servers, and firewalls.

Minimum/General Experience: Three (3) years applicable experience

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities.

Network Administrator

Functional Responsibility: Installs, configures, tests, operates, maintains, and manages networks and firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems. Ensures all network devices and configurations are compliant with current regulations and diagnose network connectivity problems. Maintains knowledge of developing, testing, and implementing network infrastructure contingency and recovery plans. Possesses experience in establishing a routing schema. Understands and performs the implementation, maintenance, and improvement of established network security practices, and installs, configures, and troubleshoots LAN and WAN components such as routers, hubs, and switches, and protects a network against malware. Knowledge of securing network communications. Possesses experience in utilizing network management tools to analyze network traffic patterns (e.g., simple network management protocol) and utilizing sub-netting tools. Skilled maintaining routers and switches (e.g. Cisco and Brocade), to include fiber channel switches in support of the SAN and DR/COOP.



Knowledge of developing and maintaining detailed network architecture and security boundary diagrams.

Minimum/General Experience: 4 years of general IT experience

Minimum Education: Bachelor's Degree or equivalent or eight (8) years overall IT experience. With a Master's Degree, three (3) years of general experience is acceptable.

Network Engineer,
Senior

Functional Responsibility: Performs design, installation, troubleshooting, and support of local- and wide-area network hardware, software and applications. Can install and configure WAN and LAN hardware. Oversees development and implementation of system specifications, designs, integration, testing, and documentation. Develops risk management and mitigation strategy. Ensures compliance with QA standards.

Minimum/General Experience: 5 years' experience in IT operations, telecommunications design, storage, and on applications involving all phases of telecommunications network design.

Minimum Education: Bachelor's Degree in related field or 8 overall years' IT experience

Network Specialist
Technician -
Intermediate

Functional Responsibility: Under general supervision, monitors and responds to technical control facility hardware and software problems utilizing hardware and software testing tools and techniques. May interface with contractor support service groups to ensure proper escalation during outages or period of degraded system performance. May assist with installation of terminals and associated hardware. May provide network server support. Requires strong knowledge of PC/Network communications hardware/software, in a multi-protocol environment, and network management software.

Minimum/General Experience: A minimum of three (3) years of professional experience in a networked environment.

Minimum Education: Requires a bachelor's degree in an associated discipline or a combination of education and experience that provides the required knowledge, skills, and abilities.

Network Support
Technician Senior

Functional Responsibility: Under general direction, monitors and responds to complex technical control facility hardware and software problems utilizing a variety of hardware and software testing tools and techniques. Provides primary interface with contractor support service groups or provides internal analysis and support to ensure proper escalation during outages or periods of degraded system performance. May provide network server support. Requires extensive knowledge of PC/network communications hardware/software in a multi-protocol environment, and network management software. May function as lead job providing guidance and training for less experienced technicians.

Minimum/General Experience: A minimum of five (5) to eight (8) years of related experience in networking environment.

Minimum Education: Requires a bachelor's degree in an associated discipline or a combination of education and experience that provides the required knowledge, skills, and abilities.

Software Engineer

Functional Responsibility: Under general supervision, performs systems analysis, evaluation, design, integration, documentation, and implementation of applications that require a thorough knowledge of administrative and technical skills.

Minimum/General Experience: Entry Level

Minimum Education: AA/ 2yr Tech School or High School Diploma/GED with 3 years' experience

Software Engineer
Intermediate

Functional Responsibility: Conducts or participates in multidisciplinary research and collaborates with equipment designers and/or hardware engineers in the planning, design, development, and utilization of electronic data processing systems software. Determines computer user needs; advises hardware designers on machine characteristics that affect software systems such as storage capacity, processing speed, and input/output requirements; designs and develops compilers and assemblers, utility programs, and operating systems. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance



phases (IV&V and DT&E). Applies higher- level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solution. May lead a team of Software Engineers.

Minimum/General Experience: 5 years' experience

Subject Matter Expert I

Minimum Education: Bachelor's Degree/equivalent or 8 years' related IT experience
Functional Responsibility: Develops and applies advanced methods, theories, and research techniques in investigating and solving complex concept, planning, design, or implementation problems. Provides technical management and direction for problem definition, analysis and requirements development and implementation for complex systems in the subject matter area. This may include defining problems and analyzes and develops plans and requirements in a subject area for complex systems. Coordinates and manages preparation of analyses, evaluations, and recommendations for proper implementation of programs and system specifications in IS architecture, automation, telecommunications, networking, communication protocols, software, email, M&S, and data storage and retrieval, etc.

Minimum/General Experience: Must have eight (8) years of Subject Matter Expertise (SME) in the respective field of services performed. At least four (4) of those years must be directly related to the required area of expertise.

Minimum Education: BA/BS or equivalent or a combination of education and experience that provides the required knowledge, skills, and abilities.

Subject Matter Expert (Journeyman)

Functional Responsibility: Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Applies principles, methods and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Minimum/General Experience: Must have five (5) years of Subject Matter Expertise (SME) in the respective field of services performed. At least two (2) of those years must be directly related to the required area of expertise.

Minimum Education: BA/BS or equivalent or a combination of education and experience that provides the required knowledge, skills, and abilities.

Subject Matter Expert (Senior)

Functional Responsibility: Serves as subject matter expert, possessing in-depth knowledge of a particular area, such as business, computer science, engineering, mathematics, or the various sciences. Provides technical knowledge and analysis of highly specialized applications and operational environments, high-level functional systems analysis, design, integration, documentation, and implementation advice on exceptionally complex problems that need extensive knowledge of the subject matter for effective implementation. Applies principles, methods, and knowledge of the functional area of capability to specific task order requirements, advanced mathematical principles and methods to exceptionally difficult and narrowly defined technical problems in engineering and other scientific applications to arrive at automated solutions.

Minimum/General Experience: Must have six (6) years of Subject Matter Expertise (SME) in the respective field of services performed. At least three (3) of those years must be directly related to the required area of expertise.

Minimum Education: BA/BS or equivalent or a combination of education and experience that provides the required knowledge, skills, and abilities.

Systems Administrator Intermediate

Functional Responsibility: Under general supervision, responsible for installing, configuring, and maintaining operating system workstations and servers, including web servers, in support of business processing requirements. Performs software installations and upgrades to operating systems and layered software packages. Schedules installations and upgrades and maintains them in accordance with established IT policies and procedures. Monitors and tunes the system to achieve optimum performance levels. Ensures workstation/server data integrity by evaluating, implementing, and



managing appropriate software and hardware solutions. Ensures data/media recoverability by implementing a schedule of system backups and database archive operations. Supports media management through internal methods and procedures or through offsite storage and retrieval services. Develops and promotes standard operating procedures. Conducts routine hardware and software audits of workstations and servers to ensure compliance with established standards, policies, and configuration guidelines. Develops and maintains a comprehensive operating system hardware and software configuration database/library of all supporting documentation.

Minimum/General Experience: A minimum of three (3) years related professional experience.

Minimum Education: Requires a bachelor's degree in the field of expertise or a combination of education and experience that provides the required knowledge, skills, and abilities.

**Systems
Administrator Level I**

Functional Responsibility: Under general supervision, provides installation, configuration, troubleshooting and maintenance of server configurations (hardware and software) to ensure their confidentiality, integrity and availability. Performs administrative and operational duties on computer systems; maintains files as required by the vendor or custom design applications; analyzes, evaluates, and tests software/hardware problems; directs installation, planning, and security of computer facilities; develops and maintains systems configuration; prepares activity and progress report regarding support activities; responds, investigates, and corrects problems; acts as a resource for all users; organizes appropriate training; utilizes commercial off-the-shelf products.

Minimum/General Experience: 4 years of general IT experience.

Minimum Education: Bachelor's Degree/equivalent or 6-years IT experience. With a Master's Degree, three (3) years of general experience is acceptable.

Systems Engineer

Functional Responsibility: Performs administration, troubleshooting and support of LAN operating systems, servers, and applications with little or no supervision.

Minimum/General Experience: Four (4) years of experience in administration of LAN operating systems, servers, and applications

Minimum Education: Associates Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities.

**Systems Engineer,
Level I**

Functional Responsibility: Performs high-level systems analysis, evaluation, design, integration, documentation, and implementation of very complex application that require a thorough knowledge of administrative and technical skills. Directs and participates in all phases of system development with emphasis on planning, analysis, evaluation, integration, testing and acceptance phases (IV&V and DT&E). Applies higher-level business or technical principles and methods to very difficult technical problems to arrive at automated engineering solutions. Designs and prepares technical reports and related documentation and makes charts and graphs to record results. Prepare and deliver presentations and briefings as required by the Task Order. May be required to serve as Team Leader.

Responsible for ensuring the quality and services delivered for particular task(s) for which this skill is performing the Team Leader position.

Minimum/General Experience: 6 years of general IT experience.

Minimum Education: Bachelor's Degree/equivalent or 9-years IT experience. With a Master's Degree, four years' of IT experience is acceptable.

**Systems Engineer,
Level II**

Functional Responsibility: Provides technical management and direction for problem definition, analysis and requirements development and implementation for complex systems in Systems Engineering. Provides recommendations and advice on system improvements, optimization and maintenance in the following areas: information systems architecture, automation, telecommunications, Networking, Communication protocols, Software, electronic Email, Modeling and Simulations, Data Storage and Retrieval, etc. May be required to serve as Task Leader.

Responsible for ensuring the quality and services delivered for particular task(s) for which this skill is



performing the Task Leader position.

Minimum/General Experience: 10 years' experience in Industry; at least 6 years directly related experience.

Minimum Education: Bachelors in related discipline or 12 years IT experience. With a Master's Degree 8 years IT experience is acceptable.

**Systems Engineer,
Senior**

Functional Responsibility: Defines and executes project systems engineering activities that may consist of systems planning, performance management, capacity planning, testing and validation, benchmarking, information engineering and systems engineering plan development and staffing.

Minimum/General Experience: A minimum of six (6) years applicable experience

Minimum Education: BA/BS or a combination of education and experience that provides the required knowledge, skills, and abilities.

**Tier I, Technical
Support II**

Functional Responsibility: Provides technical support as required in data management, document control, computer support, project control, and other related areas.

Minimum/General Experience: Three (3) years applicable experience

Minimum Education: Associates Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities. Minimum of High School diploma or equivalent.

**Tier I, Technical
Support III**

Functional Responsibility: Provides technical support as required in data management, document control, computer support, project control, and other related areas.

Minimum/General Experience: Five (5) years applicable experience

Minimum Education: Associates Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities. Minimum of High School diploma or equivalent.

**Training Specialist,
Journeyman**

Functional Responsibility: Assesses, designs, and conceptualizes training scenarios, approaches, objectives, plans, tools, aids, curriculums, and other state of the art technologies related to training and behavioral studies. Identifies the best approach training requirements to include, but not limited to hardware, software, simulations, course assessment and refreshment, assessment centers, oral examinations, interviews, computer assisted and adaptive testing, behavior-based assessment and performance, and team and unit assessment and measurement. Develops and revises training courses. Prepares training catalogs and course materials. Trains personnel by conducting formal classroom courses, workshops, and seminars.

Minimum/General Experience: Five (5) years applicable experience.

Minimum Education: Bachelor's Degree preferred or a combination of education and experience that provides the required knowledge, skills, and abilities.

Functional Responsibility: Responsible for web strategy and operations. Develops business plan and annual budget for website function. Accountable for budget, staff planning, management, and products and service delivery. Oversees operational activities of the website(s) with specific attention aimed at content creation and website maintenance.

Minimum/General Experience: 5 years' experience

Minimum Education: Bachelor's in a related discipline or 8 years IT experience.

**Web Software
Developer**

Functional Responsibility: Under general supervision, develops, codes, tests, and debugs new software and enhancements to existing web software. Competent to work on complex programs with guidance. Works with technical staff to understand problems with web software and resolve them.



Minimum/General Experience: 6 years' experience

Minimum Education: Bachelors in related discipline or 9 years IT experience. With a Master's Degree 4 years IT experience is acceptable.



Section 3. Terms and Conditions

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 54151S / 132-51)

******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 Number 132-51 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

- a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 132-51 IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.
- b. Pricing for all IT Professional Services shall be in accordance with the Contractor's customary commercial practices, e.g., hourly rates, monthly rates, term rates, and/or fixed prices, minimum general experience and minimum education.

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

EXAMPLE: Commercial Job Title: System Engineer

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



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

Minimum Education: Bachelor's Degree in Computer Science