



General Services Administration



AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST

70 - General Purpose Commercial Information Technology Equipment, Software and Services

SIN 132 51-Information Technology Professional Services – SUBJECT TO COOPERATIVE PURCHASING

FSC/PSC Class D301 IT AND TELECOM- FACILITY OPERATION AND MAINTENANCE
FSC/PSC Class D302 IT AND TELECOM- SYSTEMS DEVELOPMENT
FSC/PSC Class D306 IT AND TELECOM- SYSTEMS ANALYSIS
FSC/PSC Class D307 IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
FSC/PSC Class D308 IT AND TELECOM- PROGRAMMING
FSC/PSC Class D310 IT AND TELECOM- CYBER SECURITY AND DATA BACKUP
FSC/PSC Class D311 IT AND TELECOM- DATA CONVERSION
FSC/PSC Class D399 IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS

SIN 132 45D-Risk and Vulnerability Assessments (RVA) -- SUBJECT TO COOPERATIVE PURCHASING

FSC/PSC Class D302 IT AND TELECOM- SYSTEMS DEVELOPMENT
FSC/PSC Class D306 IT AND TELECOM- SYSTEMS ANALYSIS
FSC/PSC Class D307 IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
FSC/PSC Class D308 IT AND TELECOM- PROGRAMMING
FSC/PSC Class D310 IT AND TELECOM- CYBER SECURITY AND DATA BACKUP
FSC/PSC Class D399 IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS

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

**Mainstay Information Solutions LLC
2232 S. Randolph Street
Arlington, VA 22204
(504) 430-6101
www.mainstayis.com**

Contract Number: GS-35F-496GA

Contract Period: June 9, 2017 through June 8, 2022

**Business Size: Service Disabled Veteran Owned Small Business
Pricelist current through:**

Customer Information:

1a. Special item number(s):

Special Item Number	Description
132 51	Information Technology Professional Services
132 45D	Risk & Vulnerability Assessments (RAV)

1b. Lowest priced Item and lowest price labor category

Special Item Number	Lowest Priced Item
132 51	\$49.13
132 45D	\$49.13

1c. Labor Category Descriptions: **Please see Page 16**

2. Maximum order for SINs 132-51 and 132 45D: **\$500,000**

This maximum order threshold is a dollar amount at which it is suggested that the ordering agency request higher discounts from the contractor before issuing the order. The contractor may: (1) Offer a new lower price, (2) Offer the lowest price available under the contract, or (3) Decline the order within five (5) days. In accordance with the Maximum Order provisions contained in the Schedule, a delivery order may be placed against the Schedule contract even though it exceeds the maximum order threshold.

3. Minimum order for SIN 132-51 and 132 45D: **\$100**

4. Geographic coverage (delivery area): **Domestic delivery only**

5. Point(s) of production:

**Mainstay Information Solutions LLC
2232 S. Randolph Street
Arlington, VA 22204
(504) 430-6101**

6. Prices listed herein are net. **Please see Page 20 for more information**

7. Quantity discounts: **2% for orders over \$1M; and an additional 1% for orders over \$1.5M**

8. Prompt payment terms: **Net 30**



9a. Notification that Government purchase cards are accepted at or below the micro-purchase threshold: **Mainstay Information Solutions LLC will accept Government purchase cards at or below the micro-purchase threshold**

9b. Notification whether Government purchase cards are accepted or not accepted above the micro-purchase threshold: **Mainstay Information Solutions LLC and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold**

10. Foreign items (list items by country of origin): **N/A**

11a. Time of delivery: **Negotiated at the order level**

11b. Expedited Delivery: **Negotiated at the order level**

11c. Overnight and 2-day delivery: **Negotiated at the order level**

11d. Urgent Requirements: **Negotiated at the order level**

12. F.O.B. point(s): **FOB Destination**

13a. Ordering address:

**Mainstay Information Solutions LLC
2232 S. Randolph Street
Arlington, VA 22204
(703) 862-0078
(978) 418-0078 (Fax)**

13b. Ordering procedures: *For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3, and a sample BPA may be found at the GSA/FSS Schedule homepage (gss.gsa.gov/schedule).*

14. Payment address:

**Mainstay Information Solutions LLC
2232 S. Randolph Street
Arlington, VA 22204
(703) 862.0078
(978) 418-0078 (Fax)**



15. Warranty provision: **N/A**

16. Export packing charges, if applicable: **N/A**

17. Terms and conditions of Government purchase card acceptance: **Mainstay Information Solutions LLC will accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract. For orders with a dollar amount above the micro-purchase threshold, Mainstay Information Solutions LLC and the ordering agency may agree to use the credit card.**

18. Terms and conditions of rental, maintenance, and repair (if applicable): **N/A**

19. Terms and conditions of installation (if applicable): **N/A**

20. Terms and conditions of repair parts indicating date of parts price lists and any discounts from list prices (if applicable): **N/A**

20a. Terms and conditions for any other services (if applicable): **N/A**

21. List of service and distribution points (if applicable): **N/A**

22. List of participating dealers (if applicable): **N/A**

23. Preventive maintenance (if applicable): **N/A**

24a. Special attributes such as environmental attributes (e.g., recycled content, energy efficiency, and/or reduced pollutants): **N/A**

24b. Section 508 compliance: **If applicable, Section 508 compliance information on the supplies and services provided for under this contract are available at www.mainstayinformationsolutions.com**

25. Data Universal Number System (DUNS) number: **078446298**

26. Notification regarding registration in System for Award Management (SAM) database: **Mainstay Information Solutions LLC's SAM (System for Award Management) registration is active through November 29, 2017.**

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

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.

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)

(SPECIAL ITEM NUMBERS 132-45A, 132-45B, 132-45C and 132-45D)

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:

Vendor suitability for offering services through the Highly Adaptive Cybersecurity Services (HACS) SINs must be in accordance with the following laws and standards when applicable to the specific task orders, including but not limited to:

- **Federal Acquisition Regulation (FAR) Part 52.204-21**
- **OMB Memorandum M-06-19** - Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments
- **OMB Memorandum M -07-16** - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- **OMB Memorandum M-16-03** - Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements
- **OMB Memorandum M-16-04** – Cybersecurity Implementation Plan (CSIP) for Federal Civilian Government
- **The Cybersecurity National Action Plan (CNAP)**
- **NIST SP 800-14** - Generally Accepted Principles and Practices for Securing Information Technology Systems
- **NIST SP 800-27A** - Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- **NIST SP 800-30** - Guide for Conducting Risk Assessments

- **NIST SP 800-35** - Guide to Information Technology Security Services
- **NIST SP 800-37** - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- **NIST SP 800-39** - Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST SP 800-44** - Guidelines on Securing Public Web Servers
- **NIST SP 800-48** - Guide to Securing Legacy IEEE 802.11 Wireless Networks
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-61** - Computer Security Incident Handling Guide
- **NIST SP 800-64** - Security Considerations in the System Development Life Cycle
- **NIST SP 800-82** - Guide to Industrial Control Systems (ICS) Security
- **NIST SP 800-86** - Guide to Integrating Forensic Techniques into Incident Response
- **NIST SP 800-115** - Technical Guide to Information Security Testing and Assessment
- **NIST SP 800-128** - Guide for Security-Focused Configuration Management of Information Systems
- **NIST SP 800-137** - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- **NIST SP 800-153** - Guidelines for Securing Wireless Local Area Networks (WLANs)
- **NIST SP 800-171** - Protecting Controlled Unclassified Information in non-federal Information Systems and Organizations

1. SCOPE

- a. The labor categories, prices, terms and conditions stated under Special Item Numbers 132-45A, 132- 45B, 132-45C and 132-45D High Adaptive Cybersecurity Services apply exclusively to High Adaptive Cybersecurity Services within the scope of this Information Technology Schedule.
- b. Services under these SINs are limited to Highly Adaptive Cybersecurity Services only. Software and hardware products are under different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132- 33, 132-8), and may be quoted along with services to provide a total solution.
- c. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
- d. Highly Adaptive Cybersecurity Services provided under these SINs shall comply with all Cybersecurity certifications and industry standards as applicable pertaining to the type of services as specified by ordering agency.

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

2. ORDER

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

3. PERFORMANCE OF SERVICES

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity. All Contracts will be fully funded.
- b. The Contractor agrees to render services during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
- c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
- d. Any Contractor travel required in the performance of Highly Adaptive Cybersecurity Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts. All travel will be agreed upon with the client prior to the Contractor's travel.

4. INSPECTION OF SERVICES

Inspection of services is in accordance with 552.212-4 - CONTRACT TERMS AND CONDITIONS – COMMERCIAL ITEMS (MAY 2015) (ALTERNATE II – JUL 2009) (FAR DEVIATION – JUL 2015)(TAILORED) for Firm-Fixed Price and Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

5. RESPONSIBILITIES OF THE CONTRACTOR

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

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

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the

Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on

ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

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

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Highly Adaptive Cybersecurity Services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products.

Invoices shall be submitted monthly for recurring services performed during the preceding month.

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

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

12. DESCRIPTION OF HIGHLY ADAPTIVE CYBERSECURITY SERVICES AND PRICING

- a. The Contractor shall provide a description of each type of Highly Adaptive Cybersecurity Service offered under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D for Highly Adaptive Cybersecurity Services and it 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 Highly Adaptive Cybersecurity Services shall be in accordance with the Contractor's customary commercial practices; e.g., hourly rates, minimum general experience and minimum education.

The following is an example of the manner in which the description of a commercial job title should be presented (see SCP FSS 004)

EXAMPLE

Commercial Job Title: Computer Network Defense Analysis

Description: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Professionals involved in this specialty perform the following tasks:

- Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities
- Provide daily summary reports of network events and activity relevant to Computer Network Defense practices
- Monitor external data sources (e.g., Computer Network Defense vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of Computer Network Defense threat condition and determine which security issues may have an impact on the enterprise.

Knowledge, Skills and Abilities: Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes (e.g., in Titles 10, 18,



32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed

Minimum Experience: 5 Years

Minimum Education Requirements: a bachelor's of science degree with a concentration in computer science, cybersecurity services, management information systems (MIS), engineering or information science is essential.

Highly Desirable: Offensive Security Certified Professional (OSCP) or commercial Cybersecurity advanced certification(s).

LABOR CATEGORY DESCRIPTIONS

Labor Category	Minimum/General Experience and Years of Experience	Functional Responsibility	Educational Requirements
Technical Writer I	2-4years' experience; educational credentials may be substituted for years of experience.	Explains technical ideas in simple language. Writes technical direction on product announcements, marketing brochures, advertisements, and marketing specifications. Ensures accuracy and consistency across all written marketing content, and incorporates revisions according to current routing procedures. Defines a consistent voice and tone for the brand across multiple channels. Writes articles and reports on current trends. Submits copies to managers for feedback. Adjusts copy.	Bachelor's degree or equivalent experience.
IT Security Business Analyst I	2-4years' experience; educational credentials may be substituted for years of experience.	Demonstrates experience with the principles, methods, practices and techniques of IT Security communications. Demonstrates strong oral and written communication skills to convey detailed information on security programs, policies, and significant issues. Demonstrates experience in drafting and analyzing information security communications materials and plans. Demonstrates experience in establishing and maintaining relationships with IT security stakeholders.	Bachelor's degree or equivalent experience.
Application Tester II	4 to 6 years' experience; educational credentials may be substituted for years of experience.	Develops and executes test plans, procedures, schedules and scenarios for unit, process, function, system integration and acceptance testing. Consults with the development and/or requirements team to coordinate and test applications. Creates automated test scripts and tests existing applications for compliance with upgrades. Ensures new applications and software modifications meet requirements and operate satisfactorily in the system environment. Ensures the software interfaces with both new and existing systems. May build test environments to include configuring and installing appropriate software. Writes detailed test plans, procedures and scenarios. Documents both the successes and failures of all executed test procedures. Ensures all tools, methodologies, technologies and programming languages remain current.	Bachelor's degree or equivalent experience.
508 Compliance Tester II	4 to 6 years' experience; educational credentials may be substituted for years of experience.	Develops and maintains Section 508 compliance processes and documentation based on industry and federal government best practices and standards. Performs and/or contributes 508 testing activities for applications/systems utilizing various 508 compliance tools such as screen readers (JAWS) and URL-based testing tools (WAV). Creates, updates, and maintain application/system, integration and regression test cases. Performs full cycles of sprint, regression, and integration testing. Generates test summary reports after each testing cycle to show testing progress, actual testing results, and pass/fail status. Provides regular status updates to the Project Manager and/or development leads. Reports	Bachelor's degree or equivalent experience.



		defects and escalates issues as needed. Works closely with software development team to mitigate defects.	
Software Developer II	4 to 6 years' experience; educational credentials may be substituted for years of experience.	Reviews, analyzes, and modifies programming systems including encoding, testing, debugging and installing to support an organization's application systems. Consults with users to identify current operating procedures and to clarify program objectives. May be expected to write documentation to describe program development, logic, coding, and corrections. Writes manuals for users to describe installation and operating procedures. May lead and direct the work of others. Typically reports to a project leader or manager. Must have a working knowledge of relational databases and client-server concepts. Relies on experience and judgment to plan and accomplish goals.	Bachelor's degree or equivalent experience.
IT Security Business Analyst II	4-6 years' experience; educational credentials may be substituted for years of experience.	Demonstrates experience with the principles, methods, practices and techniques of IT Security communications. Demonstrates strong oral and written communication skills to convey detailed information on security programs, policies, and significant issues. Demonstrates experience in drafting and analyzing information security communications materials and plans. Demonstrates experience in establishing and maintaining relationships with IT security stakeholders.	Bachelor's degree or equivalent experience.
IT Security Communications Specialist II	4-6 years' experience; educational credentials may be substituted for years of experience.	Provides daily strategic communications and administrative support to Communication Manager/Project team and senior IT Security executives. Coordinates and executes outreach and engagement activities and initiatives internally with the Client/Project team and externally with program partners and stakeholders.	Bachelor's degree or equivalent experience.
IT Security Engagement Specialist II	4-6 years' experience; educational credentials may be substituted for years of experience.	Provides oversight of technical writing and editing to all phases of acquisition and technical documentation of the security program and projects. Assists with the implementation of the strategic communication plans in support of organizational security related activities. Maintains day-to-day communications with key IT security personnel and day to day efforts to track, document, and report non-compliance issues with current policies, standards, and procedures. Organizes, manages, and maintains changes of documentation repositories using a variety of collaboration tools.	Bachelor's degree or equivalent experience.
Technical Writer III	Experience: 8-10 years; educational credentials may be substituted for years of experience.	Explains technical ideas in simple language. Writes technical direction on product announcements, marketing brochures, advertisements, and marketing specifications. Ensures accuracy and consistency across all written marketing content, and incorporate revisions according to current routing procedures. Defines a consistent voice and tone for	Bachelor's degree or equivalent experience.

		the brand across multiple channels. Writes articles and reports on current trends. Submits copies to managers for feedback. Adjusts copy as necessary and proofread for grammar and spelling.	
IT Security Business Analyst III	Experience: 8-10 years; educational credentials may be substituted for years of experience.	Demonstrates experience with the principles, methods, practices and techniques of IT Security communications. Demonstrates strong oral and written communication skills to convey detailed information on security programs, policies, and significant issues. Demonstrates experience in drafting and analyzing information security communications materials and plans. Demonstrates experience in establishing and maintaining relationships with IT security stakeholders.	Bachelor's degree or equivalent experience.
IT Security Engagement Specialist III	Experience: 8-10 years; educational credentials may be substituted for years of experience.	Leads and assists in drafting information security policies, standards and procedures. Provides expert oversight of technical writing and editing to all phases of acquisition and technical documentation of the security program and projects. Assists with the implementation of the strategic communication plans in support of organizational security related activities. Maintains day-to-day communications with key IT Security personnel and day to day efforts to track, document, and report non-compliance issues with current policies, standards, and procedures. Organizes, manages, and maintains changes of documentation repositories using a variety of collaboration tools. Keeps abreast of current security technologies, trends, and industry issues to assist with the development of security articles and awareness training materials.	Bachelor's degree or equivalent experience.
Security Auditor IV	Experience: 8-10 years; educational credentials may be substituted for years of experience.	Discovers application security weaknesses, and writes recommendations for preventing or fixing them; works with the analysis and best practices for all projects. Incorporates security controls into the application which meet regulatory requirements. Assesses new and existing applications and system deployments for vulnerabilities and design flaws, and prioritizes remediation efforts based on risk.	Bachelor's degree or equivalent experience.
IT Security Business Analyst IV	Experience: 8-10 years; educational credentials may be substituted for years of experience.	Demonstrates experience with the principles, methods, practices and techniques of IT Security communications. Demonstrates strong oral and written communication skills to convey detailed information on security programs, policies, and significant issues. Demonstrates experience in drafting and analyzing information security communications materials and plans. Demonstrates experience in establishing and maintaining relationships with IT security stakeholders.	Bachelor's degree or equivalent experience
Security Engineer V	Experience: 12-15 years; educational credentials may be substituted for years of experience.	Engineer, implement and monitor security measures for the protection of computer systems, networks and information. Identifies and defines system security requirements. Designs system security architecture and develops detailed security designs. Prepares and documents standard operating procedures and protocols. Configures and troubleshoots security infrastructure devices. Develops technical solutions and new security tools to help mitigate security	Bachelor's degree or equivalent experience.

		vulnerabilities and automate repeatable tasks.	
Systems Engineer V	Experience: 12-15 years; educational credentials may be substituted for years of experience.	Manages and monitors all installed systems and infrastructure. Installs, configures, tests and maintains operating systems, application software and system management tools. Proactively ensures the highest levels of systems and infrastructure availability. Monitors and tests application performance for potential bottlenecks. Identifies possible solutions, and works with developers to implement those fixes. Maintains security, backup, and redundancy strategies. Writes and maintains custom scripts to increase system efficiency and lower the human intervention time on any tasks	Bachelor's degree or equivalent experience.

Substitute for Education Requirement Policy

Mainstay recognizes varying levels of education and experience in their position descriptions. Mainstay maintains that many times experience is as or more important than formal preparation. Therefore, it is policy to substitute two years of related experience for one year of higher education where appropriate and with the client's approval.

HOURLY RATES

Labor Category	Hourly Rate
Technical Writer I	\$48.87
IT Security Business Analyst I	\$73.30
Application Tester II	\$83.07
508 Compliance Tester II	\$83.07
Software Developer II	\$83.07
IT Security Business Analyst II	\$83.07
IT Security Communications Specialist II	\$83.07
IT Security Engagement Specialist II	\$83.07
Technical Writer III	\$97.73
IT Security Business Analyst III	\$97.73
IT Security Engagement Specialist III	\$97.73
Security Auditor IV	\$111.42
IT Security Business Analyst IV	\$112.39
Security Engineer V	\$143.67
Systems Engineer V	143.67

**USA COMMITMENT TO PROMOTE
SMALL BUSINESS PARTICIPATION
PROCUREMENT PROGRAMS**

PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

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

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

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

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

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

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

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts.



BPA NUMBER _____

**(CUSTOMER NAME)
BLANKET PURCHASE AGREEMENT**

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

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

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

(2) Delivery:

DESTINATION	DELIVERY SCHEDULES / DATES
_____	_____
_____	_____
_____	_____

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

(4) This BPA does not obligate any funds.

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

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

OFFICE	POINT OF CONTACT
_____	_____
_____	_____
_____	_____

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

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

- (a) Name of Contractor;
- (b) Contract Number;
- (c) BPA Number;
- (d) Model Number or National Stock Number (NSN);

- (e) Purchase Order Number;
- (f) Date of Purchase;
- (g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and
- (h) Date of Shipment.

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

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

BASIC GUIDELINES FOR USING “CONTRACTOR TEAM ARRANGEMENTS”

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

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

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

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

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

Here is a general outline on how it works:

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