

**GENERAL SERVICES ADMINISTRATION
AUTHORIZED FEDERAL SUPPLY SERVICE PRICELIST
INFORMATION TECHNOLOGY SCHEDULE
INFORMATION TECHNOLOGY SERVICES**

CNF Technologies is an economically disadvantaged woman owned small IT and systems engineering services firm focused on information assurance. CNF integrates proven, leading edge technologies with innovative concepts to deliver cost effective and the highest quality of engineering services and solutions. Our goal is to surpass the customer's expectations by delivering a complete package of services to meet their needs.

**Special Item Number 132-45A - HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
Penetration Testing**

Special Item Number 132-45B - HACS Incident Response

Special Item Number 132-45C – HACS Cyber Hunt

Special Item Number 132-45D – HACS Risk and Vulnerability Assessments (RVA)

- FPDS Code D301 IT and Telecom -- Facility Operation and Maintenance
- FPDS Code D302 IT and Telecom -- Systems Development
- FPDS Code D306 IT and Telecom -- Systems Analysis
- FPDS Code D307 IT and Telecom -- IT Strategy and Architecture
- FPDS Code D308 IT and Telecom -- Programming
- FPDS Code D310 IT and Telecom -- Cyber Security and Data Backup
- FPDS Code D311 IT and Telecom -- Data Conversion Services
- FPDS Code D316 IT and Telecom -- Telecommunications Network Management

Special Item Number 132-51 - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

- FPDS Code D301 IT and Telecom -- Facility Operation and Maintenance
- FPDS Code D302 IT and Telecom -- Systems Development
- FPDS Code D306 IT and Telecom -- Systems Analysis
- FPDS Code D307 IT and Telecom -- IT Strategy and Architecture
- FPDS Code D308 IT and Telecom -- Programming
- FPDS Code D310 IT and Telecom -- Cyber Security and Data Backup
- FPDS Code D311 IT and Telecom -- Data Conversion Services
- FPDS Code D316 IT and Telecom -- Telecommunications Network Management

Special Item Number 132-56 – HEALTH INFORMATION TECHNOLOGY SERVICES

- FPDS Code D301 IT and Telecom -- Facility Operation and Maintenance
- FPDS Code D302 IT and Telecom -- Systems Development
- FPDS Code D306 IT and Telecom -- Systems Analysis
- FPDS Code D307 IT and Telecom -- IT Strategy and Architecture
- FPDS Code D308 IT and Telecom -- Programming
- FPDS Code D310 IT and Telecom -- Cyber Security and Data Backup
- FPDS Code D311 IT and Telecom -- Data Conversion Services
- FPDS Code D316 IT and Telecom -- Telecommunications Network Management

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

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

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

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

General Services Administration

Federal Acquisition Service

Contract Number: GS-35F-0662V

Period Covered by Contract: Aug 24, 2014 through Aug 23, 2019

Pricelist current thru Mod # PO-0014, dated March 26, 2018

Prices Shown Herein are Net (discount deducted)

CNF Technologies Corporation
9415 Dugas Drive
San Antonio TX 78245
Office: 210.957.2800
Fax: 210.957.3089
Email: sales@cnftech.com
www.cnftech.com

Products and ordering information in this Authorized FAS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the Federal Acquisition Service's Home Page via the Internet at <http://www.fss.gsa.gov/>.

Table of Contents

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS4

TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE CYBERSECURITY SERVICES (HACS)
(SPECIAL ITEM NUMBERS 132-45A, 132-45B, 132-45C and 132-45D).....12

SINs 132-45A, 132-45B, 132-45C, and 132-45D – Highly Adaptive Cybersecurity Services (HACS) Price List
(Contractor Site)21

SINs 132-45A, 132-45B, 132-45C, and 132-45D – Highly Adaptive Cybersecurity Services (HACS) Price List
(Customer Site).....22

132-51 -- IT Professional Services Price List (Contractor Site)34

132-51 -- IT Professional Services Price List (Customer Site).....35

TERMS AND CONDITIONS APPLICABLE TO HEALTH INFORMATION TECHNOLOGY (IT) SERVICES
(SPECIAL ITEM NUMBER 132-56)36

132-56 -- Health IT (HIT) Labor Category Descriptions.....39

132-56 – Health IT (HIT) Professional Services Price List (Contractor Site)42

132-56 – Health IT (HIT) Professional Services Price List (Customer Site).....43

COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS44

BEST VALUE BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE45

BASIC GUIDELINES FOR USING — CONTRACTOR TEAM ARRANGEMENTS47

**INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS**

SPECIAL NOTICE TO AGENCIES: Small Business Participation

SBA strongly supports the participation of small business concerns in the Federal Supply Schedules Program. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micro purchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!® on-line shopping service (www.FAS.gsa.gov). The catalogs/pricelists, GSA Advantage!® and the Federal Acquisition Service Home Page (www.FAS.gsa.gov) contain information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micro purchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1. GEOGRAPHIC SCOPE OF CONTRACT:

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

Offerors are requested to check one of the following boxes:

- The Geographic Scope of Contract will be domestic and overseas delivery.
 The Geographic Scope of Contract will be overseas delivery only.
 The Geographic Scope of Contract will be domestic delivery only.

2. CONTRACTOR'S ORDERING ADDRESS AND PAYMENT INFORMATION:

**CNF Technologies Corporation
 9415 Dugas Drive
 San Antonio TX 78245**

Contractors are required to accept credit cards for payments equal to or less than the micro-purchase threshold for oral or written delivery orders. Credit cards will be acceptable for payment above the micro-purchase threshold. In addition, bank account information for wire transfer payments will be shown on the invoice.

The following telephone number(s) can be used by ordering activities to obtain technical and/or ordering assistance:

Office Phone: (210) 957-2800 Office Fax: (210) 957-3089

3. LIABILITY FOR INJURY OR DAMAGE

The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

4. STATIC DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279:

Block 9: G. Order/Modification Under Federal Schedule
 Block 16: Data Universal Numbering System (DUNS) Number: **17-1368512**
 Block 30: Type of Contractor - – A. Small Disadvantaged Business
 Block 31: Woman-Owned Small Business -**Yes**
 Block 36: Contractor's Taxpayer Identification Number (TIN): **20-1936788**

4a. CAGE Code: **34UF3**

4b. Contractor has registered with the Central Contractor Registration Database.

5. FOB DESTINATION

6. DELIVERY SCHEDULE

a. **TIME OF DELIVERY:** The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

SPECIAL ITEM NUMBERS 132-51 and 132-56 DELIVERY TIME As agreed upon between CNF Technologies and the ordering activity.

b. **URGENT REQUIREMENTS:** When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

7. **DISCOUNTS:** Prices shown are NET Prices all discounts have been incorporated into the price schedule.

- a. Prompt Payment: 0.5%-20 days
- b. Quantity: No Discount
- c. Dollar Volume: No Discount
- d. Government Educational Institutions: Government Educational Institutions are offered the same pricing as all other Government customers.
- e. Other: None

8. TRADE AGREEMENTS ACT OF 1979, as amended:

All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

9. **STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING:** None

10. **SMALL REQUIREMENTS:** The minimum dollar value of orders to be issued is 1 (one) of any labor category.

11. **MAXIMUM ORDER (All dollar amounts are exclusive of any discount for prompt payment.)**

The Maximum Order value for the following Special Item Numbers (SINs) is \$500,000:

Special Item Number 132-45A - Highly Adaptive Cybersecurity Services (HACS) - Penetration Testing

Special Item Number 132-45B - HACS Incident Response

Special Item Number 132-45C – HACS Cyber Hunt

Special Item Number 132-45 D – HACS Risk and Vulnerability Assessments (RVA)

Special Item Number 132-51 - Information Technology (IT) Professional Services

Special Item Number 132-56 – Health Information Technology Services

12. ORDERING PROCEDURES FOR FEDERAL SUPPLY SCHEDULE CONTRACTS

Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.

- a. FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.
- b. FAR 8.405-2 Ordering procedures for services requiring a statement of work.

13. FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION STANDARDS

REQUIREMENTS: Ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.

13.1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS):

Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

13.2 FEDERAL TELECOMMUNICATION STANDARDS (FED-STDS):

Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDS) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDS should be obtained from the GSA, Federal Acquisition Service, Specification Section, 470 East L'Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202)619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301)975-2833.

14. CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FAS-370) (NOV 2003)

- (a) Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

- (b) Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.
- (c) Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/ possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.
- (d) Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.
- (e) Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.
- (f) Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor's participation in such order may be restricted in accordance with FAR Part 9.5.
- (g) Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency's order.
- (h) Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency's order.
- (i) Government-Furnished Property: As specified by the agency's order, the Government may provide property, equipment, materials or resources as necessary.
- (j) Availability of Funds: Many Government agencies' operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government's obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.
- (k) Overtime: For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

15. CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES: Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See C.1.)

16. GSA ADVANTAGE!

GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors' schedule prices with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

- (1) Manufacturer; (2) Manufacturer's Part Number; and (3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (ex.: NetScape). The Internet address is <http://www.FAS.gsa.gov/>.

17. PURCHASE OF OPEN MARKET ITEMS

NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. ODCs (Other Direct Costs) are not part of this contract and should be treated as open market purchases. Ordering Activities procuring open market items must follow FAR 8.402(f).

For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, **only if-**

- (1) All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));
- (2) The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;
- (3) The items are clearly labeled on the order as items not on the Federal Supply Schedule; and
- (4) All clauses applicable to items not on the Federal Supply Schedule are included in the order.

18. CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS

a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:

- (1) Time of delivery/installation quotations for individual orders;
- (2) Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.
- (3) Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

19. OVERSEAS ACTIVITIES

The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

NONE

Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

20. BLANKET PURCHASE AGREEMENTS (BPAs)

The use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

21. CONTRACTOR TEAM ARRANGEMENTS

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

22. INSTALLATION, DEINSTALLATION, REINSTALLATION

The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of \$2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall received less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds \$2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132-8.

23. SECTION 508 COMPLIANCE.

If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following: Does not apply.

The EIT standard can be found at: www.Section508.gov/.

24. PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES.

Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order

- (a) A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and (b) The following statement:

This order is placed under written authorization from _____ dated _____. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

25. INSURANCE—WORK ON A GOVERNMENT INSTALLATION (JAN 1997)(FAR 52.228-5)

- (a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

- (b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

(1) For such period as the laws of the State in which this contract is to be performed prescribe; or (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

- (c) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

26. SOFTWARE INTEROPERABILITY.

Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at <http://www.core.gov>.

27. ADVANCE PAYMENTS

A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract. (31 U.S.C. 3324)

**TERMS AND CONDITIONS APPLICABLE TO HIGHLY ADAPTIVE
CYBERSECURITY SERVICES (HACS)
(SPECIAL ITEM NUMBERS 132-45A, 132-45B, 132-45C and 132-45D)**

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

******NOTE: All non-professional labor categories must be incidental to, and used solely to support Highly Adaptive Cybersecurity Services, and cannot be purchased separately.**

******NOTE: All labor categories under the Special Item Number 132-51 Information Technology Professional Services may remain under SIN 132-51 unless the labor categories are specific to the Highly Adaptive Cybersecurity Services SINs.**

1. SCOPE

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.

- a. 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.
- b. These SINs provide ordering activities with access to Highly Adaptive Cybersecurity services only.
- c. 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.
- d. 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

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.

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

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

9. INVOICES

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

10. RESUMES

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

11. APPROVAL OF SUBCONTRACTS

The ordering activity may require that the Contractor receive, from the ordering activity'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 following labor categories are offered under Special Item Numbers 132-45A, 132-45B, 132-45C and 132-45D for Highly Adaptive Cybersecurity.

Labor Category Descriptions – Highly Adaptive Cybersecurity Services (HACS) SIN 132-45A-D

Education Substitutions for SIN 132-45A-D Labor Categories:

Degree	Experience Equivalent
Bachelors	Associates degree plus two years' experience
Masters	Bachelors degree plus two years of experience, or Associates degree plus four years of experience
PhD/Doctorate	Masters degree plus two years of experience, or Bachelors degree plus four years of experience, or Associates degree plus six years of experience

The years of experience substituted may be used to satisfy education requirements.

Completion of higher education which has not yet resulted in a degree may be counted as one-for-one years of experience for each year of higher education and may be used to satisfy education requirements.

Experience substitutions for 132-45A-D Labor Categories:

Degree	Experience Equivalent
Masters	Two years
PhD/Doctorate	Four years

May be used to satisfy experience requirements when the minimum Education requirements are met.

Penetration Tester

Functional Responsibility:

Description: Conducts security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. May support in part or in whole technical vulnerability assessments of applications and infrastructure, vulnerability research, and generation of assessment reports. Executes tests by following the steps and procedures in a test plan and documents results in standardized format suitable for future analysis. Supports in coordination of technical tests, network scans, vulnerability scans, etc. that support the evaluation of security controls. Conducts reconnaissance data gathering and vulnerability research. Supports the creation of risk/vulnerability reporting. Leverages COTS or open source tools to conduct assessments, analyzes results, identifies exploitable vulnerabilities, and verifies vulnerabilities. Prepares and reviews assessment documents, validates and communicates key findings to stakeholders.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Risk/Vulnerability Analyst

Functional Responsibility:

Creates, reviews, and edits security risk evaluation documentation, procedures, and processes for computer networks, enterprises, applications, and weapon systems. Conducts security controls reviews for

systems under assessment. Deploys security controls and/or configuration to mitigate or address cybersecurity risk factors. Conducts vulnerability assessment of systems using COTS, GOTS or open-source tools in support of continuous monitoring of the security posture. Conducts cybersecurity risk management and information assurance in accordance with Department of Defense (DoD) Risk Management Framework (RMF) guidelines, to include testing and auditing of DoD networks, development of policy/procedure for Access and Authorization (A&A) and system operation, ultimately leading to Authorization to Operate (ATO). Audits system policies and procedures using COTS, GOTS, and open-source auditing tools. Develops plans of action and milestones to remediate cybersecurity risks and/or configuration issues. Produces, prepares, and reviews relevant documentation and validates/communicates key findings to stakeholders.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber System/Network Technician

Functional Responsibility:

Performs customer service and support for cyber systems and solutions. Answers inquiries by clarifying desired information, researching and locating information in response. Resolves problems by clarifying issues, researching and exploring answers and alternative solutions, implementing and testing solutions. Administers operating systems and/or networks in response to system documentation, manuals, or technical orders, and makes configuration changes in response to user-reported problems or trouble-tickets, or resulting from efficiency studies or other sources.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Security Engineer/Analyst

Functional Responsibility:

Participates in special projects, investigations into specific technologies/solutions, and/or researches/develops new technologies in the cyber security arena. Configures and operates development environment(s), and systems/network infrastructure required for developing sophisticated applications. Assesses, designs, develops, and recommends integrated security solutions to protect proprietary and confidential data. Provides technical and engineering services for the support of integrated systems and solutions. Interfaces with clients to translate security and mission requirements into technical requirements. Assists with configuration, validates secure complex systems, and tests/integrates security products and systems. Configures and maintains documentation, policies, etc. May develop, enhance, integrate, or sustain applications, systems, and/or solutions.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber System/Application Developer

Functional Responsibility:

Responsible for performing complex programming assignments in analyzing, defining, coding in design, and implementing cost effective cyber solutions. Develops and reviews operator and control instructions. Prepares and conducts system and programming tests. Conducts system and programming tests requiring interfacing of hardware and software. Conducts system programming activities in a variety of programming languages. Develops documentation (flow charts, processes and steps in operations, source code and documentation, inputs to technical documentation and training). May analyze system capabilities to resolve operational deficiencies or problems.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Intrusion Analyst

Functional Responsibility:

Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malware prevention, Firewalls, IDS & IPS, Web security, antispam, etc. to collect, aggregate, correlate, and fuse network security and performance data to detect potential and actual intrusions. Actively monitor cyber security threats and risks. Support defensive cyber operations and follow standard operating procedures for detecting, classifying, and reporting incidents.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Forensics/Investigator

Functional Responsibility:

Responds to crisis or urgent situations to mitigate immediate and potential threats. Coordinates with intrusion analysts, incidence response analysts, and other stakeholders to leverage cyber security information, network performance data, and threat intelligence in order to mitigate threats. Employs forensic analysis and malware exploitation tools and techniques to identify adversary capabilities, tactics, techniques, and procedures, and develop countermeasures and/or signatures to assist in enhancing the security posture of the organization. Performs both network forensics including deep packet inspection, and host-based forensics to collect evidence in accordance with standard operating procedures and guidelines established by stakeholders. May coordinate with or participate in Law Enforcement operations as required during response operations.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Incident Response Analyst

Functional Responsibility:

Performs real-time proactive event investigation on various security enforcement systems, such as SIEM, Anti-virus, Internet content filtering/reporting, malware prevention, Firewalls, IDS & IPS, Web security, antispam, etc. Contributes to generating response to crisis or urgent situations to mitigate immediate or potential threats. Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Handles and responds to cyber security incidents through coordination with stakeholders such as internal IT entities, security leadership, legal affairs, internal affairs, law enforcement, and privacy offices. Intakes incident reporting, conducts ticket updates, and notifies stakeholders of cyber security incidents and forensic investigations in relation to computer security incidents and escalates when necessary. Coordinates response to computer security incidents. Recommends courses of action on each incident and creates, manages, and records all actions taken and serve as initial POC for Events of Interest reported both internally and externally. Establishes/implements alarm/alert/incident escalation process and tracks, follows-up, and resolves incidents.

Minimum/General Experience and Education:

Junior: Associates Degree and a minimum of 0-4 years of experience

Intermediate: Bachelors Degree and a minimum of 3-7 years of experience

Senior: Bachelors Degree and minimum of 5-9 years of experience

Subject Matter Expert: Advanced degree and 7-11 years of experience

Cyber Program/Project Manager

Functional Responsibility:

Responsible for planning and executing project. Prepares and maintains the project schedule and budget; performs overall technical/cost/schedule management, monitoring and reporting. Ensures that work on the program is carried out in accordance with the appropriate Government specifications, procedures, and standards. Serves as primary point of contact with the Government. Directs efforts of other managers and staff. Conducts in-process reviews, status reviews, monthly project status reviews, and bi-weekly program reviews. Approves/accepts Government tasking. Authorizes work activity, expenditure or procurement. Submits formal monthly status reports. Functions as final QA checkpoint for program activities.

Minimum/General Experience and Education:

Junior: B.Sc. in Computer Science, Engineering, or related technical degree and 6 – 10 total years of experience in cyber or equivalent area (engineering, software development, information technology, etc.) and minimum 4 years experience managing delivery teams and projects.

Intermediate: B.Sc. in Computer Science, Engineering, or related technical degree and 8 – 12 total years of experience in cyber or equivalent area (engineering, software development, information technology, etc.) and minimum 6 years of experience managing delivery teams and projects.

Senior: B.Sc. in Computer Science, Engineering, or related technical degree and 10-15 total years of experience in cyber or equivalent area (engineering, software development, information technology, etc.) and minimum 8 years of experience managing delivery teams and projects.

Cyber Configuration/Quality Assurance Specialist

Functional Responsibility:

Reports to PM in staff role (independent/objective). Coordinates with other managers on quality issues. Attends program reviews. Develops, implements, reviews quality assurance program for compliance with Government standards. Prepares/revises program QA plan/procedures. Performs formal QA of services provided. Monitors work efforts/deliverables for quality.

Minimum/General Experience and Education:

B.Sc. in Computer Science (or equivalent technical/engineering degree). Five years of experience in Quality Assurance or Configuration Management, with 2 years of experience in process, application, system, or software development.

Cyber Technical Writer/Editor

Functional Responsibility:

Responsible for documentation design, development, and preparation throughout the production cycle that can include: technical writing/editing, editorial consultation, copy design/editing, proofreading, or overall documentation review. Works with management, technical personnel, authors, and subject matter experts to define documentation content, guidelines, specifications, and development schedules. Prepares required documentation in an appropriate format. Adheres to configuration management/quality assurance standards.

Minimum/General Experience and Education:

Bachelor's degree in Communications, Journalism, English, or a related field. Five years of experience in writing, designing, editing, and preparing business or technical documentation. Experience with and demonstrated knowledge of Department of Defense (DoD), Federal Information Processing (FIP), Government Printing Office (GPO), or commercial documentation standards as appropriate to the assignment.

- b.** Pricing for all Highly Adaptive Cybersecurity Services, Contractor Site and Customer Site, are on the following pages.

THIS SECTION INTENTIONALLY LEFT BLANK

**SINs 132-45A, 132-45B, 132-45C, and 132-45D – Highly Adaptive
Cybersecurity Services (HACS) Price List (Contractor Site)**

Contractor Site	
Labor Category	Mar-18
Penetration Tester, Junior	\$84.46
Penetration Tester, Intermediate	\$121.64
Penetration Tester, Senior	\$128.99
Penetration Tester, SME	\$136.12
Cyber Risk/Vulnerability Analyst, Junior	\$72.22
Cyber Risk/Vulnerability Analyst, Intermediate	\$90.57
Cyber Risk/Vulnerability Analyst, Senior	\$107.61
Cyber Risk/Vulnerability Analyst, SME	\$128.81
Cyber System/Network Technician, Junior	\$63.55
Cyber System/Network Technician, Intermediate	\$86.32
Cyber System/Network Technician, Senior	\$104.08
Cyber System/Network Technician, SME	\$126.28
Cyber Security Engineer/Analyst, Junior	\$84.46
Cyber Security Engineer/Analyst, Intermediate	\$95.78
Cyber Security Engineer/Analyst, Senior	\$126.28
Cyber Security Engineer/Analyst, SME	\$136.12
Cyber System/Application Developer, Junior	\$77.99
Cyber System/Application Developer, Intermediate	\$103.87
Cyber System/Application Developer, Senior	\$126.28
Cyber System/Application Developer, SME	\$136.12
Cyber Intrusion Analyst, Junior	\$90.11
Cyber Intrusion Analyst, Intermediate	\$94.44
Cyber Intrusion Analyst, Senior	\$103.53
Cyber Intrusion Analyst, SME	\$126.28
Cyber Forensics/Investigator, Junior	\$95.78
Cyber Forensics/Investigator, Intermediate	\$111.72
Cyber Forensics/Investigator, Senior	\$126.28
Cyber Forensics/Investigator, SME	\$136.12
Cyber Incident Response Analyst, Junior	\$95.78
Cyber Incident Response Analyst, Intermediate	\$111.72
Cyber Incident Response Analyst, Senior	\$126.28
Cyber Incident Response Analyst, SME	\$131.53
Cyber Program/Project Manager, Junior	\$98.63
Cyber Program/Project Manager, Intermediate	\$114.11
Cyber Program/Project Manager, Senior	\$136.12
Cyber Configuration/ Quality Assurance Specialist	\$84.83
Cyber Technical Writer/Editor	\$60.71

**SINs 132-45A, 132-45B, 132-45C, and 132-45D – Highly Adaptive
Cybersecurity Services (HACS) Price List (Customer Site)**

Customer Site	
Labor Category	Mar-18
Penetration Tester, Junior	\$ 71.83
Penetration Tester, Intermediate	\$ 103.42
Penetration Tester, Senior	\$ 109.68
Penetration Tester, SME	\$ 115.75
Cyber Risk/Vulnerability Analyst, Junior	\$ 61.42
Cyber Risk/Vulnerability Analyst, Intermediate	\$ 77.02
Cyber Risk/Vulnerability Analyst, Senior	\$ 91.52
Cyber Risk/Vulnerability Analyst, SME	\$ 109.53
Cyber System/Network Technician, Junior	\$ 54.02
Cyber System/Network Technician, Intermediate	\$ 73.40
Cyber System/Network Technician, Senior	\$ 88.51
Cyber System/Network Technician, SME	\$ 107.40
Cyber Security Engineer/Analyst, Junior	\$ 71.83
Cyber Security Engineer/Analyst, Intermediate	\$ 81.46
Cyber Security Engineer/Analyst, Senior	\$ 107.40
Cyber Security Engineer/Analyst, SME	\$ 115.75
Cyber Systems/Application Developer, Junior	\$ 66.31
Cyber Systems/Application Developer, Intermediate	\$ 88.32
Cyber Systems/Application Developer, Senior	\$ 107.40
Cyber Systems/Application Developer, SME	\$ 115.75
Cyber Intrusion Analyst, Junior	\$ 76.60
Cyber Intrusion Analyst, Intermediate	\$ 80.32
Cyber Intrusion Analyst, Senior	\$ 88.03
Cyber Intrusion Analyst, SME	\$ 107.40
Cyber Forensics/Investigator, Junior	\$ 81.46
Cyber Forensics/Investigator, Intermediate	\$ 95.00
Cyber Forensics/Investigator, Senior	\$ 107.40
Cyber Forensics/Investigator, SME	\$ 115.75
Cyber Incident Response Analyst, Junior	\$ 81.46
Cyber Incident Response Analyst, Intermediate	\$ 95.00
Cyber Incident Response Analyst, Senior	\$ 107.40
Cyber Incident Response Analyst, SME	\$ 111.84
Cyber Program/Project Manager, Junior	\$ 83.87
Cyber Program/Project Manager, Intermediate	\$ 97.02
Cyber Program/Project Manager, Senior	\$ 115.75
Cyber Configuration/ Quality Assurance Specialist	\$ 72.13
Cyber Technical Writer/Editor	\$ 51.62

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

NOTE: All non-professional labor categories must be incidental to, and used solely to support professional services, and cannot be purchased separately. Further, non-professional labor categories shall be offered under SIN 132 100 only.

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. I-FSS-60 PERFORMANCE INCENTIVES (APR 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-
- (3) 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
 - (4) 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/EC SERVICES AND PRICING

CNF Technologies is an IT Professional and systems engineering services firm focused on information assurance. CNF integrates proven, leading edge technologies with innovative concepts to deliver cost effective and the highest quality professional services. CNF assists customers implement, operate, secure, and manage their network enterprises. The CNF team possesses extensive experience in network defense, intrusion detection, vulnerability assessments, patch management, incident response, and forensic analysis. CNF principals have significant expertise evaluating and integrating emerging technologies; designing secure architectures; rapid prototyping; and performing vulnerability assessments and penetration tests.

- a.** The following labor categories are offered under Special Item Number 132-51 IT Professional Services.

Program Manager

Minimum/General Experience:

Combination of 15 years of experience in an engineering discipline, including 8 years of experience in the management of very large and complex information technology projects.

Functional Responsibility:

Responsible for planning and executing project. Prepares and maintains the project schedule and budget; performs overall technical/cost/schedule management, monitoring and reporting. Ensures that work on the program is carried out in accordance with the appropriate Government specifications, procedures, and standards. Serves as primary point of contact with the Government. Directs efforts of other managers and staff. Conducts in-process reviews, status reviews, monthly project status reviews, and bi-weekly program reviews. Approves/accepts Government tasking. Authorizes work activity, expenditure or procurement. Submits formal monthly status reports. Functions as final QA checkpoint for program activities.

Minimum Education:

Bachelor's degree in an Engineering/Computer Science discipline or a related field. With a Master's degree, 13 years of experience in information technology is required.

Program Support Specialist

Minimum/General Experience:

Two years of experience assisting a Project/Program Manager in the management of a contract, project, or task. Requires knowledge of and experience using specialized financial and project tracking software systems in addition to commercial off-the-shelf (COTS) office automation software packages.

Functional Responsibility:

Responsible for providing management assistance for planning and executing a project. Assist the Project/Program Manager during the preparation and maintenance of project schedules and budgets. Prepares and delivers status reports or reviews. Tracks staffing, budget, prioritization, and other personnel matters for the Project/Program Manager.

Minimum Education:

Bachelor's degree in Business or a related field.

Configuration/Quality Assurance Specialist

Minimum/General Experience:

Five years of experience in Quality Assurance or Configuration Management, with 2 years of experience in process, application, system, or software development.

Functional Responsibility:

Reports to PM in staff role (independent/objective). Coordinates with other managers on quality issues. Attends program reviews. Develops, implements, reviews quality assurance program for compliance with Government standards. Prepares/revises program QA plan/procedures. Performs formal QA of services provided. Monitors work efforts/deliverables for quality.

Minimum Education:

Bachelor's degree in Engineering/Computer Science or a related field.

Technical Writer/Editor

Minimum/General Experience:

Five years of experience in writing, designing, editing, and preparing business or technical documentation.

Experience with and demonstrated knowledge of Department of Defense (DoD), Federal Information Processing (FIP), Government Printing Office (GPO), or commercial documentation standards as appropriate to the assignment.

Functional Responsibility:

Responsible for documentation design, development, and preparation throughout the production cycle that can include: technical writing/editing, editorial consultation, copy design/editing, proofreading, or overall documentation review. Works with management, technical personnel, authors, and subject matter experts to define documentation content, guidelines, specifications, and development schedules. Prepares required documentation in an appropriate format. Adheres to configuration management/quality assurance standards.

Minimum Education:

Bachelor's degree in Communications, Journalism, English, or a related field.

Associate Systems/Network Engineer

Minimum/General Experience:

Two years of experience related to a specific engineering or computer science discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communications systems or networks.

Exposure to, or familiarity with, Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

Provides supervised support for routine activities, according to established procedures or instructions. Supports the installation, testing, maintenance, and troubleshooting of operational systems or networks. Assists with technical support for elements such as: complex processes, applications, systems, software, networks, satellites, telecommunications, facilities, or machinery. Support assistance can include, but is not limited to, elements such as: research, studies, requirements/specifications definition, analysis, assessments, planning, acquisition, design, development, integration, overseeing, testing, installation, performance tuning, operation, deployment, or maintenance. Interfaces with users during the support process and may support user training. Contributes to technical documentation. Uses basic elements of applicable methodologies, modeling/estimating techniques, tools, applications, systems, software, or databases to perform assigned tasks. Complies with the standards and organization requirements.

Minimum Education:

Bachelor's degree in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

Systems/Network Engineer

Minimum/General Experience:

Five years of experience related to a specific engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communication systems or networks.

Familiarity with Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

Provides support for work that is varied and somewhat difficult, but that involves limited responsibility. Supports the installation, testing, maintenance, and troubleshooting of operational systems or networks. Manages a variety of system/network support functions, including trouble ticket management, service order entry, and/or configuration management. Provides technical support for elements such as: complex processes, equipment, applications, systems, software, networks, satellites, telecommunications, facilities, or machinery. Support can include, but is not limited to, elements such as: research, studies, requirements/specifications definition, analysis, assessments, planning, acquisition, design, development, integration, overseeing, testing, installation, performance tuning, operation, deployment, or maintenance. Interfaces with users during the support process and may support user training. Develops/prepares technical documentation. Uses applicable methodologies, modeling/estimating techniques, tools, applications, systems, software, or databases to perform assigned tasks. Ensures compliance with the standards. May provide staff/project supervision.

Minimum Education:

Bachelor's degree in Engineering, Computer Science, Information Systems, Math, Physics or other engineering related discipline.

Senior Systems/Network Engineer

Minimum/General Experience:

Eight years of experience related to a specific, engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of telecommunication systems or networks. Extensive operational experience with Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

Supports the planning, analysis, design, testing, and troubleshooting of networks or operational systems. Provides comprehensive technical support and/or leadership for elements such as: complex processes, applications, systems, software, networks, satellites, telecommunications, facilities, or machinery. Performs and/or leads project planning, scope, control, management, tracking, or review activities. Support includes, but is not limited to, elements such as: research, studies, requirements/specifications definition, analysis, assessments, planning, acquisition, design, development, integration, overseeing, testing, installation, performance tuning, operation, deployment, or maintenance. Interfaces with users at all levels during the support process. Performs and/or leads technical document development/preparation. Uses applicable methodologies, modeling/estimating techniques, tools, applications, systems, software, or databases at advanced levels to perform assigned tasks. Ensures compliance with, and/or may develop, the standards and organization requirements relative to VA cyber security. May supervise or manage tasks/projects.

Minimum Education:

Bachelor's degree in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

Associate Systems Analyst/Developer

Minimum/General Experience:

Two years of technical experience in applications software development, one of which is in systems analysis. Competent to work at a high technical level for most phases of applications systems analysis and

programming activities. Two years of experience in the development of Internet/intranet applications such as home pages, interfaces with databases, and security. Proficient with HyperText Markup Language (HTML), JAVA, or other Internet/intranet application engines as required. Two years of technical experience in administration, analysis, and programming of computerized databases. Competent to work in most phases of database management.

Functional Responsibility:

Works under close direction. Formulates/defines system scope and objectives. Devises or modifies procedures to solve moderately complex problems considering computer equipment capacity and limitations. Codes, tests, debugs, and documents computer programs. Participates in related areas, such as database design, implementation, integration, management, and maintenance, and evaluation of commercial off-the-shelf (COTS) products.

Minimum Education:

Bachelor's degree in Computer Science, Software Engineering, or a related field.

Systems Analyst/Developer

Minimum/General Experience:

Five years of technical experience in applications software development, three of which are in systems analysis, and 1 year of which is acting as technical lead for a team of developers. Has a good understanding of the business or function for which the application is designed. Six years of experience in the development of Internet/intranet applications such as home pages, interfaces with databases, and security. Proficient with HyperText Markup Language (HTML), JAVA, or other Internet/intranet application engines as required. Six years of technical experience in administration, analysis, and programming of computerized databases. Competent to work at a high level for all phases of system/database development/management.

Functional Responsibility:

Works under general direction. Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations. Prepares detailed specifications from which programs will be written. Designs, codes, tests, debugs, and documents programs. Participates in related areas, such as design, implementation, integration, management, and maintenance of complex databases, with respect to the operating system, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, guidelines, and statistical methods; evaluation of commercial off-the-shelf (COTS) products; and analysis of network hardware/software issues. provides guidance to other developers.

Minimum Education:

Bachelor's degree in Computer Science, Software Engineering, or a related field.

Senior Systems Analyst/Developer

Minimum/General Experience:

Eight years of technical experience in applications software development, three of which are in systems analysis, and 3 years of which is acting as technical lead for a team of developers. Has a good understanding of the business or function for which the application is designed. Six years of experience in the development of Internet/intranet applications such as home pages, interfaces with databases, and security. Proficient with HyperText Markup Language (HTML), JAVA, or other Internet/intranet application engines as required. Six years of technical experience in administration, analysis, and

programming of computerized databases. Competent to work at a high level for all phases of system/database development/management.

Functional Responsibility:

Plans, directs and monitors the work of team members. Sets priorities to meet the needs of users. Formulates/defines system scope and objectives. Devises or modifies procedures to solve complex problems considering computer equipment capacity and limitations. Prepares detailed specifications from which programs will be written. Designs, codes, tests, debugs, and documents those programs. Participates in related areas, such as such as design, implementation, integration, management, and maintenance of complex databases, with respect to the operating system, access methods, access time, device allocation, validation checks, organization, protection and security, documentation, guidelines, and statistical methods; evaluation of commercial off-the-shelf (COTS) products; and analysis of network hardware/software issues. Directs the work of other developers. This skill is qualified to operate in advanced technical environments that include C++, Client/Server, Oracle, PowerBuilder, Visual Basic, JAVA, and other source code requirements.

Minimum Education:

Bachelor's degree in Computer Science, Software Engineering, or a related field.

Associate Security Analyst**Minimum/General Experience:**

Two years of experience in performing operating and analyzing computer systems and networks. Experience in configuring Commercial off-the-shelf (COTS) software to operate on specific hardware. Experience in performing simple routine technical tasks using detailed procedures and under close supervision.

Functional Responsibility:

Receives telephone calls or electronic reports and responds to inquiries and requests for assistance from users having specific computer and network problems. Reports and tracks network and system problems. Resolves simple computer software and hardware problems. Transfers tasks to other IT groups to resolve more complex problems.

Minimum Education:

High School Diploma/GED

Security Analyst**Minimum/General Experience:**

Four years experience in performing computer and network operations. Experience in configuring and installing software applications to operate on specific hardware. Experience in performing routine engineering tasks and analysis using procedures and under general supervision.

Functional Responsibility:

Monitors computer and network traffic. Analyzes network traffic activity and system logs to determine cause of problem. Reports and tracks network and system problems. Resolves simple computer software and hardware problems. Coordinates with other IT groups to resolve more complex problems.

Minimum Education:

High School Diploma/GED. With an Associate's Degree in Engineering/Computer Science or related field, 2 years of functional experience is required.

Senior Security Analyst

Minimum/General Experience:

Six years experience in performing computer and network operations. Experience in configuring and troubleshooting software applications to operate on specific hardware. Experience in performing highly technical tasks and analysis.

Functional Responsibility:

Evaluates the security posture of computers and networks. Responds to network and system intrusive activity. Analyzes network traffic and system logs to determine corrective action. Implements countermeasures and operates security tools. Performs remote maintenance of security agents, sensors, tools, and systems. Monitors and responds to complex technical hardware and software problems utilizing a variety of tools and techniques. Acts as the interface with vendor support service groups.

Minimum Education:

High School Diploma/GED. With an Associate's Degree in Engineering/Computer Science or related field, 4 years of functional experience is required.

Associate Systems/Network Administrator

Minimum/General Experience:

Three years experience in administrating Windows operating systems. Experience in installing and configuring Windows operating software to operate on specific hardware. Experience in performing simple routine tasks using existing procedures and under close supervision.

Functional Responsibility:

Performs preventive maintenance, troubleshooting, and repair of computer systems and peripheral equipment. Responsible for maintaining an adequate spare parts inventory. May maintain network hardware. May configure software applications to operate on specific hardware. Monitors and responds to simple hardware and software problems utilizing a variety of testing tools and techniques. May provide server support.

Minimum Education:

High School Diploma/GED. With an Associate's Degree in Engineering/Computer Science Discipline or related industry certifications, 1 year of functional experience is required.

Systems/Network Administrator

Minimum/General Experience:

Four years experience in administrating Windows, Unix, and Linux operating systems and servers. Experience in configuring networks, network components, and protocol analysis. Experience in configuring and troubleshooting system and network administration tools.

Functional Responsibility:

Performs preventive maintenance, troubleshooting, and repair of computer and network systems. Configures and troubleshoots software applications to operate on specific hardware. Monitors and responds to technical hardware and software problems utilizing a variety of testing tools and techniques. Acts as the interface with vendor support service groups. Provides internal analysis and support to ensure proper escalation during outages or periods of degraded system performance. Provide server support. Oversees other system administrators.

Minimum Education:

High School Diploma/GED. With an Associates Degree in Engineering/Computer Science Discipline or related industry certifications, 2 years of functional experience is required.

Subject Matter Expert**Minimum/General Experience:**

Ten years of specialized technical experience in a functional area of expertise.

Functional Responsibility:

Provides expert consultative support to a functional technical area of the project. Develops solutions to complex problems. Works closely with the engineers to identify the best technological solution to technical issues. Provides expert guidance and direction at the expert and intellectual levels for very difficult areas requiring innovation, research, or for tasks involving information technologies related policy at a high level affecting large organizations or enterprises.

Minimum Education:

Master's degree in a relevant functional area. With a Bachelor's degree in Engineering/Computer Science Discipline or related field, 12 years of functional experience is required.

Senior Subject Matter Expert**Minimum/General Experience:**

Twelve years of specialized technical experience in a functional area of expertise.

Functional Responsibility:

Provides expert consultative support to a functional technical area of the project. Develops solutions to complex problems. Works closely with the engineers to identify the best technological solution to technical issues. Provides expert guidance and direction at the highest possible expert and intellectual levels for very difficult areas requiring innovation, research, or for tasks involving information technologies related policy at the highest level affecting large organizations or enterprises.

Minimum Education:

Master's degree in a relevant functional area. With a Bachelor's degree in Engineering, Computer Science Discipline or related field, 14 years of functional experience is required.

- b.** Pricing for labor categories offered under Special Item Number 132-51 IT Professional Services, Contractor Site and Customer Site, are on the following pages.

**132-51 -- IT Professional Services Price List
(Contractor Site)**

Contractor Site	
Labor Category	Nov-17
Program Manager	\$102.26
Program Management Specialist	\$65.97
Configuration/Quality Assurance Specialist	\$85.77
Technical Writer/Editor	\$61.57
Associate System/Network Engineer	\$62.67
System/Network Engineer	\$89.07
Senior System/Network Engineer	\$105.55
Associate Systems Analyst/Developer	\$58.27
Systems Analyst/Developer	\$84.67
Senior Systems Analyst/Developer	\$105.55
Associate Security Analyst	\$49.48
Security Analyst	\$60.48
Senior Security Analyst	\$73.68
Associate System/Network Administrator	\$68.17
System/Network Administrator	\$79.17
Subject Matter Expert	\$120.96
Senior Subject Matter Expert	\$151.74

**132-51 -- IT Professional Services Price List
 (Customer Site)**

Contractor Site	
Labor Category	Nov-17
Program Manager	\$85.77
Program Management Specialist	\$54.98
Configuration/Quality Assurance Specialist	\$72.57
Technical Writer/Editor	\$52.78
Associate System/Network Engineer	\$53.88
System/Network Engineer	\$74.77
Senior System/Network Engineer	\$90.16
Associate Systems Analyst/Developer	\$47.28
Systems Analyst/Developer	\$71.47
Senior Systems Analyst/Developer	\$87.96
Associate Security Analyst	\$41.79
Security Analyst	\$51.68
Senior Security Analyst	\$61.57
Associate System/Network Administrator	\$57.18
System/Network Administrator	\$65.97
Subject Matter Expert	\$103.36
Senior Subject Matter Expert	\$131.95

**TERMS AND CONDITIONS APPLICABLE TO
HEALTH INFORMATION TECHNOLOGY (IT) SERVICES
(SPECIAL ITEM NUMBER 132-56)**

NOTE: This SIN is limited to professional Health IT Services only. Any non-professional labor categories shall be offered under SIN 132 100 only. All non-professional labor categories must be incidental to, and used solely to support Health IT services, and cannot be purchased separately.. Software and hardware products are out of scope.

1. SCOPE

- a. The labor categories, prices, terms, and conditions stated under Special Item Number 132-56 Health Information Technology Services apply exclusively to Health IT Services within the scope of this Information Technology Schedule.
- b. This SIN is limited to Health IT Services only. Software and hardware products are out of scope. Hardware and software can be acquired through different Special Item Numbers on IT Schedule 70 (e.g. 132-32, 132-33, 132-8).
- c. This SIN provides ordering activities with access to Health IT services.
- d. Health IT Services provided under this SIN shall comply with all Healthcare certifications and industry standards as applicable at the task order level.
- 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 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 Health 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. All travel will be agreed upon with the client prior to the Contractor's travel.

4. 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.

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 (Dec 2007) Rights in Data – General, may apply.

6. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

7. INDEPENDENT CONTRACTOR

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

8. ORGANIZATIONAL CONFLICTS OF INTEREST

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

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

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

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule

contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.

9. INVOICES

The Contractor, upon completion of the work ordered, shall submit invoices for Health 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.

10. RESUMES

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

11. INCIDENTAL SUPPORT COSTS

Incidental support costs are not considered part of 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.

12. 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.

13. DESCRIPTION OF HEALTH IT SERVICES AND PRICING

CNF Technologies is an IT and systems engineering services firm focused on information assurance. CNF integrates proven, leading edge technologies with innovative concepts to deliver cost effective and the highest quality professional services. CNF assists customers implement, operate, secure, and manage their network enterprises. The CNF team possesses extensive experience in network defense, intrusion detection, vulnerability assessments, patch management, incident response, and forensic analysis. CNF principals have significant expertise evaluating and integrating emerging technologies; designing secure architectures; rapid prototyping; and performing vulnerability assessments and penetration tests for Health Information Technology activities.

- a.** The following labor categories are offered under Special Item Number 132-51 IT Professional Services.

132-56 -- Health IT (HIT) Labor Category Descriptions

HIT Systems Administrator:

Minimum General Experience:

3-5 years of experience in administrating Windows, Unix, and Linux operating systems and servers. Experience in configuring networks, network components, and protocol analysis. Experience in configuring and troubleshooting system and network administration tools.

Functional Responsibility:

A HIT System Administrator has the thorough knowledge to create plans to assure effective management, operations, and maintenance of health IT systems and/or networks. Manages teams of system admins and is able to prioritize work and identify high risk critical problems and dedicate appropriate resources. Has extensive knowledge of a wide variety of systems and networks to include high volume/high availability systems.

Minimum Education:

BS/AS in Engineering/Computer Science Discipline or related industry certifications.

HIT Network Engineer:

Minimum General Experience:

3-5 years of experience related to a specific engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communication systems or networks. Familiarity with Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

A HIT Network Engineer plans, supports and evaluates network systems and makes recommendations for resources required to maintain and/or expand service levels concerning health IT systems. Also provides and develops technical standards and interface applications; identifies and evaluates new products; provide solutions for network problems. Provide monthly metrics for network availability and bandwidth usage as well as other metrics as requested. Uses network management tools to discover, map and maintain the network. Responsible for network equipment OS and version upgrades. Monitor and maintain network interfaces to insure its highest level of performance and makes modifications and enhancements as needed. Responsible for documenting procedures and keeping network diagrams and related material up to date. Handles initial user problems, questions, and request on network issues.

Minimum Education:

BS in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

HIT Senior Network Engineer:

Minimum General Experience:

8+ years of experience related to a specific engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communication systems or networks. Familiarity with Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

A HIT Senior Network Engineer plans, supports and evaluates complex existing network systems and make recommendations for resources required to maintain and/or expand service levels concerning health IT systems. This resource will provide highly skilled technical assistance in network planning, engineering and architecture. Also provides and develops technical standards and interface applications; identifies and evaluates new products; provide solutions for network problems. Interfaces with internal/external customers and vendors to determine system needs. Plans and incorporates how new network resources and applications will exist on the network. Provide monthly metrics for network availability and bandwidth usage as well as other metrics as requested. Responsible for network capacity planning. Use network management tools to discover, map and maintain the network. Responsible for network equipment OS and version upgrades. Responsible for conducting research of new technologies and implementation strategies. Monitor and maintain network interfaces to insure its highest level of performance and makes modifications and enhancements as needed. Responsible for documenting procedures and keeping network diagrams and related material up to date. Handle escalated user problems, questions, and request on network issues. Work with other groups within IS to resolve network related issues as needed. Leads and directs work of other Network Engineers.

Minimum Education:

MS/BS in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

HIT Subject Matter Expert/Program Manager:**Minimum Experience/Education:**

Requires 10 years of experience in direct program management and 10 years of progressive engineering experience.

Functional Responsibility:

A HIT Program Manager should have experience with diverse health IT projects both large and small. Should be well versed in full systems development life cycle, enterprise wide network engineering, strategic information planning, business process reengineering, structure and management practices. Should be able to identify and mitigate risks to the program. Should be able to manage to cost, schedule and performance.

A HIT Subject Matter Expert should have extensive experience in the coordination of program and project leaders to identify requirements for system architecture concerning health IT systems. Should be able to identify strategies for addressing requirements. Should have extensive experience with analysis of requirements against fiscal, schedule, and performance issues. Has extensive experience in taking program requirements and is able to create an architecture vision having experience in high volume and high availability networks and systems. Experience in creating and conveying to team members the architectural vision for a program or project. Is responsible for dictating design choices to software developers, including but not limited to: platforms, coding and technical levels. Experience in establishing and enforcing standards and practices. Overseeing the development team, he manages the full life cycle of the software development process. Has extensive software development experience and thorough knowledge of a variety of programming languages and logic.

Minimum Education:

A MS/BS degree in Computer Science, Information Systems, or relevant technical, engineering, or scientific field.

HIT Cyber Security Engineer:**Minimum General Experience:**

3-5 years of experience related to a specific, engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of HIT systems or networks.

Functional Responsibility:

A HIT Cyber Security Engineer has IT experience in multiple aspects of Cyber Security with intermediate experience with healthcare oriented IT systems involving end user as well as enterprise level networks. Experience in designing and implementing systems that meet agency Cyber Security policy and regulations. Ideally has experience in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks.

Minimum Education:

BS in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

HIT Sr. Cyber Security Engineer:**Minimum General Experience:**

8+ years of experience related to a specific, engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of complex, heterogeneous systems or networks.

Functional Responsibility:

A HIT Sr. Cyber Security Engineer has extensive IT experience in all aspects of Cyber Security with a vast array of healthcare oriented IT systems involving end user as well as enterprise level networks. Experience in designing and implementing systems that meet agency Cyber Security policy and regulations. Should have extensive experience in Cyber Security Tools, network topologies, intrusion detection, PKI, and secured networks.

Minimum Education:

MS/BS in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

HIT Configuration/Release Manager:**Minimum General Experience:**

3-5 years of experience related to a specific engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communication systems or networks.

Functional Responsibility:

A HIT Configuration/Release Manager should have experience and be able to develop, document, and implement detailed plans for ensuring configuration control for health related IT programs, projects, and tasks. When issues arise, should be able to identify and implement solutions. Maintain thorough records and documentation to ensure accurate product builds, part ordering and product and/or software updates. Should have experience in management of individual releases of software, hardware or other system components. Should have experience in coordinating with QA, Development, packaging and hardware

teams. The release manager should have experience in documenting releases, risks and in maintaining the schedule of planned releases.

Minimum Education:

BS/AS in Engineering/Computer Science Discipline or related industry certifications.

HIT Integration Engineer:

Minimum General Experience:

8+ years of experience related to a specific engineering or computer science, discipline such as: communications engineering, electrical engineering, or electronics engineer in support of communication systems or networks. Familiarity with Government or industry processes, procedures, standards, methodologies, and tools.

Functional Responsibility:

A HIT Integration Engineer should have experience in the creation of strategies and plans for integration of multiple health IT systems/subsystems into an operational unit, ensuring full functional and performance capabilities are retained. The integration engineer should be experienced in introducing new hardware or software into a new or existing environment while minimizing disruption and mitigating risks

Minimum Education:

BS in Engineering, Computer Science, Information Systems, Math, Physics, or other engineering related discipline.

- b. The following tables include pricing for labor categories offered under Special Item Number 132-56 Health IT Services, Contractor Site and Customer Site.

**132-56 – Health IT (HIT) Professional Services Price List
(Contractor Site)**

<i>Contractor Site</i>	
Labor Category	Jul-17
HIT System Administrator	\$87.42
HIT Network Engineer	\$92.29
HIT Senior Network Engineer	\$105.40
HIT Subject Matter Expert/HIT Program Manager	\$136.14
HIT Cybersecurity Engineer	\$98.34
HIT Senior Cyber Security Engineer	\$119.31
HIT Configuration/Release Manager	\$79.20
HIT Integration Engineer	\$121.00

**132-56 – Health IT (HIT) Professional Services Price List
(Customer Site)**

<i>Customer Site</i>	
Labor Category	Jul-17
HIT System Administrator	\$75.61
HIT Network Engineer	\$79.83
HIT Senior Network Engineer	\$91.18
HIT Subject Matter Expert/HIT Program Manager	\$117.77
HIT Cybersecurity Engineer	\$85.06
HIT Senior Cyber Security Engineer	\$103.21
HIT Configuration/Release Manager	\$68.51
HIT Integration Engineer	\$104.67

THIS SECTION INTENTIONALLY LEFT BLANK

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

PREAMBLE

CNF Technologies Corporation provides commercial products and services to ordering activities. As an economically disadvantaged woman owned small business, 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. To accelerate potential opportunities please contact: **Contracting Phone: (210) 957-2800, E-mail: contracting@cnftech.com, Fax: (210) 957-3089.**

**BEST VALUE
BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE**

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) GS-35F-0662V.

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

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

Signatures

Ordering Activity Date

Contractor Date

BPA NUMBER _____

(CUSTOMER NAME)
BLANKET PURCHASE AGREEMENT

Pursuant to GSA Federal Supply Schedule Contract Number(s) GS-35F-0662V, 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 of 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 customer's 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.