Leneer Data Assurance Solutions, Inc. is pleased to be able to provide professional support services in the area IT Professional Services.

Special Item No. 54151S - Information Technology Professional Services
ANCILLARY – Ancillary Supplies and Services
NEW - Introduction of New Supplies and Services

SPECIAL ITEM NUMBER 54151S - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES
FPDS Code D301  IT Facility Operation and Maintenance
FPDS Code D302  IT Systems Development Services
FPDS Code D306  IT Systems Analysis Services
FPDS Code D307  Automated Information Systems Design and Integration Services
FPDS Code D308  Programming Services
FPDS Code D310  IT Backup and Security Services
FPDS Code D311  IT Data Conversion Services
FPDS Code D313  Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) Services
FPDS Code D316  IT Network Management Services
FPDS Code D317  Creation/Retrieval of IT Related Automated News Services, Data Services, or Other Information Services (All other information services belong under Schedule 76)
FPDS Code D399  Other Information Technology Services, Not Elsewhere Classified

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

Note 2: Offerors and Agencies are advised that the Group 70 – Information Technology 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.

Leneer Data Assurance Solutions, Inc.
2625 Blair Stone Rd.
Tallahassee, FL 32301
(301)476-1844

Contract Number: GS-35F-570AA
Period Covered by Contract: March 31, 2021 – September 23, 2023
Table of Contents

Information for Ordering Activities.................................................................................................................. 4
Terms and Conditions Applicable to Information Technology Professional Services (Special Item Number (SIN) 54151S).......................................................................................................................10
IT Professional Services Labor Category Descriptions...................................................................................... 14
Price List For IT Professional Services........................................................................................................... 27
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 Acquisition Service. 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 micropurchase 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!™ online shopping service (www.gsaadvantage.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Acquisition Service Home Page (www.fss.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 micropurchase 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.
[X] The Geographic Scope of Contract will be domestic delivery only.

2. CONTRACTOR’S ORDERING ADDRESS AND PAYMENT INFORMATION:

a. Ordering Address
Leneer Data Assurance Solutions, Inc.
2625 Blair Stone Rd.
Tallahassee, FL 32301

Email: info@leneer.net

b. Payment Address
Leneer Data Assurance Solutions, Inc.
1801 McCormick Drive, Suite 350
Largo, MD 20603
Contractor will accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract. The Contractor and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold (See GSAR 552.232-79 Payment by Credit Card). 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: (301)476-1844 ext 102

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. STATISTICAL 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: 825887420 |
| Block 30: | Type of Contractor - Small Disadvantaged Business |
| Block 31: | Woman-Owned Small Business - (NO) |
| Block 36: | Contractor's Taxpayer Identification Number (TIN): 26-446018 |

4a. CAGE Code: 54HQ3

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:

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Special Item Numbers</td>
<td>Determined at task level</td>
</tr>
</tbody>
</table>

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:

a. Prompt Payment: 1%, 10 days; .5%, 15 days
b. Quantity: None.
c. Dollar Volume: None
d. Government Educational Institutions: None.
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:
Not available within the scope of this contract

10. Small Requirements: The minimum dollar value of an order for delivery to one destination is $3,000.

11. MAXIMUM ORDER (All dollar amounts are exclusive of any discount for prompt payment.)
a. The Maximum Order value for the following Special Item Numbers (SINs) is $500,000:
   Special Item Number 54151S - Information Technology Professional Services
b. The Maximum Order value for the following Special Item Numbers (SINs) is $250,000:
   ANCILLARY – Ancillary Supplies and Services
   NEW - Introduction of New Supplies and 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-FSS-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 52.212-4).

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.gsaadvantage.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
   Not available under the scope 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 552.237-74, 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 or 132-9.

23.  SECTION 508 COMPLIANCE.
   I certify that in accordance with 508 of the Rehabilitation Act of 1973, as amended (U.S.C. 794d), FAR 39.2 and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR 1194) General Services Administration (GSA), that all IT hardware/software/ are 508 compliant:

   Yes X  No ___
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)
1. **SCOPE**
   a. The prices, terms and conditions stated under Special Item Number 54151S Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
   b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

   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 incurring of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

(1) Cancel the stop-work order; or

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

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

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

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

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

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

6. INSPECTION OF SERVICES

The Inspection of Services–Fixed Price (AUG 1996) (Deviation 1 – May 2003) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (May 2001) (Deviation 1 – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour 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 (Deviation – 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 (OCT 2008) (ALTERNATE I – OCT 2008) (DEVIAITON 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 (OCT 2008) (ALTERNATE I – OCT 2008) (DEVIAITON I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
(b) The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
   (1) The offeror;
   (2) Subcontractors; and/or
   (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

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

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

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

16. DESCRIPTION OF IT PROFESSIONAL SERVICES AND PRICING
a. The Contractor shall provide a description of each type of IT Service offered under Special Item Numbers 132-51 IT Professional Services should be presented in the same manner as the Contractor sells to its commercial and other ordering activity customers. If the Contractor is proposing hourly rates, a description of all corresponding commercial job titles (labor categories) for those individuals who will perform the service should be provided.

b. Pricing for all IT Professional Services shall be in accordance with the Contractor’s customary commercial practices; e.g., hourly rates, monthly rates, term rates, and/or fixed prices.
LABOR CATEGORY DESCRIPTIONS

IT Program Manager
Responsibilities
Serves as the interface with the client’s senior management personnel, and program managers, as required, to successfully meet program objectives. Maintains liaison and direction of lower level managers, business and technical staff. Leads cross-functional business, management or technical teams; using staff effectively; employing management and engineering skills to achieve program results. Directs senior level staff in developing cost projections, controlling and reporting cost, formulating and enforcing work standards, assigning staff work schedules, reviewing and resolving work discrepancies, supervising personnel, and communicating policies, purposes, and goals of the organization to subordinates and subcontractors.

Basic Qualifications
Experience in managing multi-disciplinary programs/projects.

IT Project Manager
Responsibilities
Serves as Project Manager for a large, complex task order (or a group of task orders affecting the same common/standard/migration system) and shall assist the Program Manager in working with the Government Contracting Officer (CO), the contract-level Contracting Officer’s Representative (COR), the task order level COR(s), government management personnel and customer agency representatives. Responsible for the overall management of the specific task order(s) and insuring that the technical solutions and schedules in the task order are implemented in a timely manner. Performs enterprise wide horizontal integration planning and interfaces to other functional systems. Directs completion of tasks within estimated timeframes and budget constraints.

Basic Qualifications
Twelve years of relevant experience that provides the required knowledge and skills. Advanced degree desired.

Junior IT Project Manager
Responsibilities
Prepares project management administrative plans and reports. Performs analysis, development, and review of program administrative operating procedures. Manages technical, financial, contract administration, other specialty functions and scheduling activities of the program or project for the program or project manager. Reviews and provides input to reports and other contract deliverables under a project. Utilizes experience in project and cost management tools and software for use in tracking project progress. Provides demonstrated knowledge and understanding of information technology project (and IT aspects of Facility Management) responsibilities for the execution of work under the contract. Oversees
other administrative support personnel providing direct support to information technology projects. Services of this labor category are only available through this schedule in a support role of the principal information technology positions.

**Basic Qualifications**

- Four (4) years of increasingly responsible management, IT or related work experience.
- Two (2) years of experience as a lead project manager and/or supervisor in support of a multifunctional, integrated information environment with multiple applications, or a client wide solution.

**Systems/Business Analyst**

**Responsibilities**

- Reports to, and receives task assignments from, the Contractor's Project Manager for the design and development of litigation support, imaging, web and web applications, management, workflow, or economic analysis systems;
- Defines system requirements using standard systems analysis techniques in conjunction with client systems analysts, senior technical managers, economists and other end users;
- Develops specifications for system design, data base structures, data capture forms, data conversion procedures, data validation/correction steps, and data base query and reporting procedures;
- Implements information systems through the use of data base management systems, statistical packages, high level programming languages, standard utilities and job control languages. Builds logical and physical data base structures. Develops programs for the entry, modification, validation, conversion and loading of data. Develops programs and procedures to facilitate query and reporting from data bases. Develops programs and procedures for maintenance and back-up of data base files;
- Provides oral and written status reports to the Contractor's on-site Project Manager;
- Recommends and implements enhancements to client system development procedures, software and application systems;
- Provides effective technical direction and supervision to analysts and programmers assigned to work on application development tasks;
- Provides end user and technical documentation and training for all systems developed. Provides technical training in the use of system development tools selected by the client to develop their Apps (Exp: ORACLE, SQL, JAVA, Visual Tools, associated Web technologies DBMS backend DBMS tools) but strictly as dependent on client App environment(s).

**Basic Qualifications**

- Six years of general data processing experience;
Two years of task leadership, and quality assurance experience;

Experience as noted below in the analysis, design, implementation or support of application systems using the appropriate disciplines.

Senior Security Engineer

Responsibilities

Works independently to provide information security direction and consultation to project organizations in support of complex IT projects. Reviews client information technology security procedures, strategies and standards and identifies specific areas of vulnerability. Analyzes vulnerabilities and recommends procedural and/or IT infrastructure improvements. Plans and implements recommended IT infrastructure improvements. Analyzes industry-wide trends, laws, and standards as they related to security and recommends methods, procedures, and products to solve information security problems. Leads the development of information security publications and standard operating procedures.

Basic Qualifications

Twelve (12) years of specialized experience in information technology design, development and implementation in addition to two (2) years’ experience working on complex IT security solutions.

Principal Information Systems Risk Management Analyst

Responsibilities

Perform system security analyses on company and client networks and automated information systems (AIS); provide guidance, training, research, and recommendations on client networks and AIS; perform security audits, evaluations, and risk assessments of complex operational data processing communications systems and facilities and provide recommendations for countering detected vulnerabilities; conduct security and internal control reviews of sensitive applications software; conduct specific technical reviews to support non-standard operational requirements and systems; design, develop, and maintain unique security tools and techniques for conducting computer and communications security evaluations and risk assessments; provide advanced technical computer and communications security assistance; provide expert assistance and recommendations in the field of trusted computer systems and networks; conduct security tests, certifications, and evaluations of applications and systems processing sensitive or classified information; develop requirements and specifications for reviewing and approving procurement requests, major systems development activities, telecommunications and teleprocessing hardware and software, and hardware and software encryption techniques on the basis of security concerns; and assess technology to ensure that security vulnerabilities are identified and countered.

Basic Qualifications
Eleven (11) to fifteen (15) years’ experience or equivalent education in network/systems management and operation, including communication systems operations analyses on a variety of hardware/software architectures; experience in system analysis and design (both functional and security); experience in software analysis and implementation; in-depth knowledge of information systems vulnerabilities and associated security requirements; extensive UNIX and NT experience; extensive experience in LAN and WAN network architectures, and communications and connectivity protocols; hands-on experience in information system technical specifications and design, and information systems operations; experience in performing comprehensive assessments of information systems (including stand-alone PCs, LAN/WANs, Internet/on-line access, communications connectivity, encryption devices, firewalls, hardware, software, procedures, and security measures) to detect information system security vulnerabilities. Must have ability to program in high-level languages such as C, C++, Pascal, etc. Must have experience with database tools. Must have excellent verbal and written communications skills, and must possess excellent presentation skills. Must be familiar with project management.

**Senior Information Systems Risk Management Analyst**

**Responsibilities**

Under limited supervision perform system security analyses on company and client networks and automated information systems (AIS); provide guidance, training, research, and recommendations on client networks and AIS; perform security audits, evaluations, and risk assessments of complex operational data processing communications systems and facilities and provide recommendations for countering detected vulnerabilities; conduct security and internal control reviews of sensitive applications software; conduct specific technical reviews to support non-standard operational requirements and systems; assist in the design, development, and maintenance of unique security tools and techniques for conducting computer and communications security evaluations and risk assessments; provide technical computer and communications security assistance; provide expert assistance and recommendations in the field of trusted computer systems and networks; conduct security tests, certifications, and evaluations of applications and systems processing sensitive or classified information; assist in the development of requirements and specifications for reviewing and approving procurement requests, major systems development activities, telecommunications and teleprocessing hardware and software, and hardware and software encryption techniques on the basis of security concerns; and assess technology to ensure that security vulnerabilities are identified and countered.

communications connectivity, encryption devices, firewalls, hardware, software, procedures, and security measures) to detect information system security vulnerabilities. Must have ability to program in high-level languages such as C, C++, Pascal, etc. Must have experience with database tools. Must have excellent verbal and written communications skills.

**Basic Qualifications**

Eight (8) to twelve (12) years experience or equivalent education in network/systems management and operation, including communication systems operations analyses on a variety of hardware/software architectures; experience in system analysis and design (both functional and security); experience in software analysis and implementation; knowledge of information systems vulnerabilities and associated security requirements; UNIX and NT experience; experience in LAN and WAN network architectures, and communications and connectivity protocols; hands-on experience in information system technical specifications and design, and information systems operations; experience in performing assessments of information systems (including stand-alone PCs, LAN/WANs, Internet/on-line access, communications connectivity, encryption devices, firewalls, hardware, software, procedures, and security measures) to
detect information system security vulnerabilities. Must have ability to program in high-level languages such as C, C++, Pascal, etc. Must have experience with database tools. Must have excellent verbal and written communications skills.

**Risk Management Specialist**

**Responsibilities**

Assists in the conduct of surveys of client processes, operations, and infrastructure to identify critical information that must be protected; the identification of hostile threats to and vulnerabilities of client processes, operations and infrastructure; the performance of risk assessments of client activities using proprietary tools; and in the development and implementation of mitigation measures.

**Basic Qualifications**

Five (5) years’ experience or equivalent education in program protection analysis, protection planning, and program implementation. Requires experience in OPSEC to include OPSEC surveys, identification of critical information, threat assessment, vulnerability assessment, risk assessment, and development of mitigation measures (countermeasures). Requires familiarity with decision science and decision support tools and limited analytical experience.

**System Security Engineer (I-V)**

**Responsibilities**

Advises customer and/or performs tasks to insure cost-effective system design and development, with integrated/embedded security features that are compliant with required certification/accreditation standards.

**Basic Qualifications**

At least five (5) years’ experience in engineering design or system security specification and analysis, and integration of system security features into developmental programs. Strong AIS Security skills. Current SSBI may be required.

**Mid-Level Security Specialist**

**Responsibilities**

Advises customer and/or performs tasks to develop and monitor security standards and compliance in fields of personnel, physical, technical or AIS security.

**Basic Qualifications**

At least two (2) years’ experience in security support processes and four (4) years experience in appropriate market sector/environment to be secured. Current SSBI may be required.
Network Security Engineer IV

Responsibilities

To perform a full range of systems security accreditation and certification tasks, to engineer IDS, firewall, SIM, and vulnerability scan solutions, specific experience is required to address responsibilities in the following functional areas:

- Administer network security, network design and integration as needed;
- Assess network, server and data base security requirements and vulnerabilities against NIST standards;
- Baseline analysis and documentation of existing security infrastructure, policies and procedures;
- Performing and documenting risk assessments, analyzing security vulnerabilities, and the metrics to measure the risks associated with those vulnerabilities;
- Manage dedicated network infrastructures which link the backup and data transfer segments in each computer facility;
- Comprehensive support for application developer staff as may be needed;
- Based on the risk profile of the analyzed systems, development and documentation of Contingency Plans for ameliorating those risks;
- Design, development and documentation of comprehensive Systems Security Plans, covering at a high level the infrastructure, policies and procedures which define the systems security profile for the analyzed systems;
- Development of Security Features Users Guides specific to selected networks, desktop computers, servers & data base systems;
- Design, development, and validation of System Test and Evaluation (ST&E) reviews for new and/or legacy systems.
- Development of specific policies and procedures for compliance with FISMA and FISCAM requirements and best practices for systems security controls in such areas as system development life cycle, configuration management, change management, separation of duties, software architecture, and software library management. In addition to these duties a level IV Network Engineer - Information Security is an advisory Consultant to both government and commercial clients to assist in defining needs, projection milestones for achieving goals, and to identify the approach along with each phase and level of effort. Activities to include performing a full range of systems security accreditation and certification tasks, to engineering IDS, firewall, SIM, and vulnerability scan solutions, specific experience is required.

Basic Qualifications

- Nine years of general data processing experience;
- Two or more years task/project leadership experience and four years working to apply quality assurance concepts and procedures;
Five or more years’ experience performing network engineering and analysis, assessment, auditing or related support using the appropriate disciplines. Experience with these systems is to be allocated as follows:

- Security assessments with related documentation, security upgrades of live networks, desktop systems, servers, and associated enterprise databases working closely with Infosec Auditors and Analyst leading to successful accreditation and certification of the network and related systems.
- Experience with security requirements and vulnerabilities against FISMA, and NIST standards;
- Experience developing specific policy and procedure for compliance with FISMA and FISCAM requirements;
- Experience performing full security certification and accreditation functions as defined in the Overview Table-03 of “Network Engineer - Information Security (Perform security C&A functions);”
- Experience developing requirements for, evaluating, installing, documenting policies and procedures, executing and monitoring items of the Overview Table-04 of “Products, Tools & Processes” and with using and/or assessing as many of the network “products & tools” in this same table as a candidate’s skills allow time to assimilate and support.

Information Assurance Analyst I

Responsibilities

Conduct assessment of MIS systems security requirements, evaluate current security posture and recommend priorities for remediation in preparation for IG audits.

- review MIS infrastructure and application architecture
- assess security requirements
- review existing certification and accreditation (C&A) documentation
- system policies, procedures and controls
- security infrastructure (e.g., IDS, firewalls, vulnerability scan tools)
- recommend specific areas for additional work in order by priority
- develop policies and procedures based on best practices for addressing weaknesses identified.

Evaluate and strengthen standard MIS C&A Documentation:

- Performing and documenting risk assessments, analyzing security vulnerabilities, and the metrics to measure the risks associated with those vulnerabilities;
• Based on risk profile of an analyzed system, development and documentation of Contingency Plans for ameliorating the risks;

• Design, development and documentation of comprehensive Systems Security Plan, covering at a high level the infrastructure, policies and procedures which define the systems security profile for the analyzed systems;

• Development of Security Users Guides specific to selected networks, desktop computers, servers and data base systems;

• Design, development, and validation of System Test and Evaluation (ST&E) reviews for new and/or legacy systems.

• In summary, specific C&A documents to be reviewed and strengthened include:
  • Systems Security Plan
  • Security Features Users Guide
  • Risk Assessment
  • Contingency Plan
  • Incident Response Plan
  • System Test and Evaluation

**Basic Qualifications**

• Four years of general data processing experience;

• Introductory work with systems quality assurance concepts and procedures;

The experience noted as follows in the analysis, assessment, auditing or related support using the appropriate disciplines.

• One year plus of solid experience working with a senior Infosec Analyst to perform system security assessments (i.e., ST&E), documentation, and security upgrades for live networks, desktop systems, servers, and enterprise data bases preparing for accreditation and certification (i.e., C&A) of such systems. Experience in System Development Life Cycle (i.e., SDLC) components for security, engineering and financial applications using IV&V, IDEF, proof-of-concept structuring, prototyping, code development, requirements decomposition, and documentation reviews.

• One year plus of solid experience working with a senior Infosec Analyst in the functional areas in use of and/or working familiarity with systems and standards.

**Information Assurance Analyst II**

**Responsibilities**
Conduct assessment of MIS systems security requirements, evaluate current security posture and recommend priorities for remediation in preparation for IG audits.

- review MIS infrastructure and application architecture
- assess security requirements
- review existing certification and accreditation (C&A) documentation
- system policies, procedures and controls
- security infrastructure (e.g., IDS, firewalls, vulnerability scan tools)
- recommend specific areas for additional work in order by priority
- develop policies and procedures based on best practices for addressing weaknesses identified.

Evaluate and strengthen standard MIS C&A Documentation:

- Performing and documenting risk assessments, analyzing security vulnerabilities, and the metrics to measure the risks associated with those vulnerabilities;
- Based on risk profile of an analyzed system, development and documentation of Contingency Plans for ameliorating the risks;
- Design, development and documentation of comprehensive Systems Security Plan, covering at a high level the infrastructure, policies and procedures which define the systems security profile for the analyzed systems;
- Development of Security Users Guides specific to selected networks, desktop computers, servers and data base systems;
- Design, development, and validation of System Test and Evaluation (ST&E) reviews for new and/or legacy systems.
- In summary, specific C&A documents to be reviewed and strengthened include:
  - Systems Security Plan
  - Security Features Users Guide
  - Risk Assessment
  - Contingency Plan
  - Incident Response Plan
  - System Test and Evaluation

Basic Qualifications
Six years of general data processing experience;

- One year of experience working to apply quality assurance concepts and procedures;
- Experience noted as follows in the analysis, assessment, auditing or related support using the appropriate disciplines.
- Two years of experience performing systems security assessments, documentation, and security upgrades for live networks, desktop systems, servers, and enterprise data bases leading to successful accreditation and certification of such systems.
- Experience in System Development Life Cycle components for security, engineering and financial applications using IV&V, IDEF, proof-of-concept structuring, prototyping, code development, requirements decomposition, and documentation reviews.

**Information Assurance Analyst III**

**Responsibilities**

Conduct assessment of MIS systems security requirements, evaluate current security posture and recommend priorities for remediation in preparation for IG audits.

- review MIS infrastructure and application architecture
- assess security requirements
- review existing certification and accreditation (C&A) documentation
- system policies, procedures and controls
- security infrastructure (e.g., IDS, firewalls, vulnerability scan tools)
- recommend specific areas for additional work in order by priority
- develop policies and procedures based on best practices for addressing weaknesses identified.

Evaluate and strengthen standard MIS C&A Documentation:

- Performing and documenting risk assessments, analyzing security vulnerabilities, and the metrics to measure the risks associated with those vulnerabilities;
- Based on risk profile of an analyzed system, development and documentation of Contingency Plans for ameliorating the risks;
- Design, development and documentation of comprehensive Systems Security Plan, covering at a high level the infrastructure, policies and procedures which define the systems security profile for the analyzed systems;
- Development of Security Users Guides specific to selected networks, desktop computers, servers and data base systems;
- Design, development, and validation of System Test and Evaluation (ST&E) reviews for new and/or legacy systems.
In summary, specific C&A documents to be reviewed and strengthened include:

- Systems Security Plan
- Security Features Users Guide
- Risk Assessment
- Contingency Plan
- Incident Response Plan
- System Test and Evaluation

**Basic Qualifications**

- Seven years of general data processing experience;
- One or more years of task leadership experience, and two or more years experience working to apply quality assurance concepts and procedures;
- Experience noted as follows in the analysis, assessment, auditing or related support using the appropriate disciplines. Experience with those client required systems;
- Three or more years of experience performing systems security assessments, documentation, and security upgrades for live networks, desktop systems, servers, and enterprise data bases leading to successful accreditation and certification (i.e., C&A) of such systems.
- Experience in System Development Life Cycle (i.e., SDLC) components for security, engineering and financial applications using IV&V, IDEF, proof-of-concept structuring, prototyping, code development, requirements decomposition, and documentation reviews.
- Three or more years’ experience in the following functional areas in use and familiarity with the systems and standards.

**Information Assurance Analyst IV**

**Responsibilities**

Conduct assessment of MIS systems security requirements, evaluate current security posture and recommend priorities for remediation in preparation for IG audits.

- review MIS infrastructure and application architecture
- assess security requirements
- review existing certification and accreditation (C&A) documentation
- system policies, procedures and controls
- security infrastructure (e.g., IDS, firewalls, vulnerability scan tools)
- recommend specific areas for additional work in order by priority
• develop policies and procedures based on best practices for addressing weaknesses identified.

Evaluate and strengthen standard MIS C&A Documentation:

• Performing and documenting risk assessments, analyzing security vulnerabilities, and the metrics to measure the risks associated with those vulnerabilities;

• Based on risk profile of an analyzed system, development and documentation of Contingency Plans for ameliorating the risks;

• Design, development and documentation of comprehensive Systems Security Plan, covering at a high level the infrastructure, policies and procedures which define the systems security profile for the analyzed systems;

• Development of Security Users Guides specific to selected networks, desktop computers, servers and data base systems;

• Design, development, and validation of System Test and Evaluation (ST&E) reviews for new and/or legacy systems.

• In summary, specific C&A documents to be reviewed and strengthened include:
  • Systems Security Plan
  • Security Features Users Guide
  • Risk Assessment
  • Contingency Plan
  • Incident Response Plan
  • System Test and Evaluation

Basic Qualifications

• Eight years of general data processing experience;

• Two years of task/project leadership, and three years’ experience working to apply quality assurance concepts and procedures; Experience as noted below in the analysis, assessment, auditing or related support using the appropriate disciplines.

Experience with these systems is to be allocated as follows:

• Four years of experience performing systems security assessments, documentation, and security upgrades for live networks, desktop systems, servers, and enterprise data bases leading to successful accreditation and certification of such systems.
• Experience in System Development Life Cycle components for security, engineering and financial applications using IV&V, IDEF, proof-of-concept structuring, prototyping, code development, requirements decomposition, and documentation reviews.

• Four years’ experience in the following functional areas in use of and/or working familiarity with the systems and standards.
## 54151S – IT Professional Services

<table>
<thead>
<tr>
<th>Labor Category</th>
<th>Rate/Hr</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Program Manager</td>
<td>$161.20</td>
</tr>
<tr>
<td>IT Project Manager</td>
<td>$154.15</td>
</tr>
<tr>
<td>Jr. IT Project Management Professional</td>
<td>$110.00</td>
</tr>
<tr>
<td>Systems/Business Analyst</td>
<td>$100.00</td>
</tr>
<tr>
<td>Senior Security Engineer</td>
<td>$160.00</td>
</tr>
<tr>
<td>Principal Information Systems Risk Management Analyst</td>
<td>$160.00</td>
</tr>
<tr>
<td>Senior Information System Risk Management Analyst</td>
<td>$160.00</td>
</tr>
<tr>
<td>Risk Management Specialist</td>
<td>$160.00</td>
</tr>
<tr>
<td>System Security Engineer (I-V)</td>
<td>$160.00</td>
</tr>
<tr>
<td>Mid-Level Security Specialist</td>
<td>$120.00</td>
</tr>
<tr>
<td>Network Security Engineer IV</td>
<td>$145.08</td>
</tr>
<tr>
<td>Information Assurance Analyst I</td>
<td>$84.63</td>
</tr>
<tr>
<td>Information Assurance Analyst II</td>
<td>$96.72</td>
</tr>
<tr>
<td>Information Assurance Analyst III</td>
<td>$120.00</td>
</tr>
<tr>
<td>Information Assurance Analyst IV</td>
<td>$128.96</td>
</tr>
</tbody>
</table>
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION
PROCUREMENT PROGRAMS

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

COMMITMENT
To actively seek and partner with small businesses.
To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.
To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.
To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small businesses to supply products and services to our company.
To inssure 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 (Abdullah Baytops, President and CEO, (301) 861-3099, abdul@thedigitalcorp.com).