



LUNARLINE COMMERCIAL CATALOG (2011-2012)

(Valid until May 18, 2012)

INFORMATION TECHNOLOGY SERVICES HOURLY LABOR RATES & TRAINING COURSES

(Current as of May 18, 2011)

Lunarline, Inc.
3300 North Fairfax Drive, Suite 308
Arlington, VA 22201
Telephone: (571) 481-9300
Fax: (202) 315-3003
Web: www.lunarline.com

Special Item Numbers:
132-50 Training Courses
132-51 Information Technology Professional Services

General Services Administration
Authorized IT Schedule Price List
Federal Supply Service Schedule 70
**General Purpose Commercial Information Technology
Equipment, Software, and Services**

Contract Number: **GS-35F-0392X**
Contract Period: **MAY 18, 2011 – May 17, 2016**

SIN 132-51 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 D308	Millennium Conversion Services (Y2K)
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	Automated News Services, Data Services, or Other Information Services
FPDS Code D399	Other Information Technology Services, Not Elsewhere Classified

Lunarline, Inc.
3300 North Fairfax Drive, Suite 308 Arlington, VA 22201
Phone (571) 481-9300

<http://www.lunarline.com>

Contract Number: GS-35F-0392X

Period Covered by Contract: 05/18/2011 – 05/17/2016

General Services Administration
Federal Acquisition Service

Products and ordering information in this Authorized FSS 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.gsaadvantage.gov/>.

TABLE OF CONTENTS

1. Geographic Scope of Contract.....	3
2. Contractor’s Ordering Address and Payment Information.....	3
3. Liability for Injury or Damage	5
4. Statistical Data for Government Ordering Office Completion of Standard Form 279.....	5
5. FOB Destination	5
6. Delivery Schedule.....	5
7. Discounts: Prices Shown are Net Prices; Basic Discounts Have Been Deducted.....	5
8. Trade Agreements Act of 1979, as Amended.....	5
9. Statement Concerning Availability of Export Packing	6
10. Small Requirements.....	6
11. Maximum Order (All dollar amounts are exclusive of any discount for prompt payment.).....	6
12. Use of Federal ACQUISITION Services Information Technology Schedule Contracts, In Accordance With FAR 8.404	6
13. Federal Information Technology/Telecommunication Standards Requirements	7
14. Security Requirements.....	8
15. Contract Administration for Ordering Offices	8
16. GSA Advantage!.....	8
17. Purchase of Open-Market, Non-Schedule Items	8
18. Contractor Commitments, Warranties, and Representations.....	9
19. Overseas Activities	9
20. Blanket Purchase Agreements (BPAS)	9
21. Contractor Team Arrangements	10
22. Installation, Deinstallation, Reinstallation.....	10
23. Section 508 Compliance	10
TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51).....	11
1. Scope.....	11
2. Performance Incentives	11
3. Ordering Procedures for Services (Requiring a Statement of Work).....	11
4. Order.....	13
5. Performance of Services	13
6. Inspection of Services.....	14
7. Responsibilities of the Contractor	14
8. Responsibilities of the Government.....	14
9. Independent Contractor	14
10. Organizational Conflicts of Interest.....	14
11. Invoices.....	14

12. Payments..... 15

13. Resumes..... 15

14. Open Market Costs..... 15

15. Approval of Subcontracts..... 15

16. Description of IT Services and Pricing..... 15

17. BEST VALUE BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE..... 16

18. BLANKET PURCHASE AGREEMENT..... 17

19. Lunarline Professional Labor Category Descriptions..... 19

20. Lunarline Training Course Descriptions..... 30

INFORMATION FOR ORDERING OFFICES 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 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.fss.gsa.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

The geographic scope of this contract is the 48 contiguous states, the District of Columbia, Alaska, Hawaii, the Commonwealth of Puerto Rico, and such other overseas locations as listed herein.

2. Contractor's Ordering Address and Payment Information

Ordering Address:

Lunarline, Inc.
3300 North Fairfax Drive, Suite 308
Arlington, VA 22201


Payment Address:

Lunarline, Inc.
3300 North Fairfax Drive, Suite 308
Arlington, VA 22201

Contractors are required to accept the Government purchase card for payments equal to or less than the micro-purchase threshold for oral or written delivery orders. Government purchase 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 agencies to obtain technical and/or ordering assistance:

1 (571) 481-9300



3. Liability for Injury or Damage

The Contractor shall not be liable for any injury to Government personnel or damage to Government 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: GS-35F-0392X

Block 16: Data Universal Numbering System (DUNS) Number: 14-718-1569

Block 30: Type of Contractor:

A. Service Disabled Veteran Owned Business

Block 36: Contractor's Taxpayer Identification Number (TIN): 56-245-8165

4a. CAGE Code: 3WNE8

4b. Contractor has registered with the Central Contractor Registration Data Base.

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 NUMBER	DELIVERY TIME (Days ARO)
<u>132-50, 132-51</u>	<u>30</u> Days

b. URGENT REQUIREMENTS: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering agency, agencies 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 agency, 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; Basic Discounts Have Been Deducted

- a. Prompt Payment: 1 % – 20 days from receipt of invoice or date of acceptance, whichever is later.
- b. Quantity – 1% discount on SIN 152-150 orders from \$100,000-499,000 and 3% on orders greater than \$500,000
- d. Government Educational Institutions are offered the same discounts as all other Government customers.
- e. Other – 0% discount

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

10. Small Requirements

The minimum dollar value of orders to be issued is \$25,000.00.

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 132-51 – Information Technology (IT) Professional Services
- b. The Maximum Order value for the following Special Item Numbers (SINs) is \$25,000:
Special Item Number 132-50 – Training Services

12. Use of Federal ACQUISITION Services Information Technology Schedule Contracts, In Accordance With FAR 8.404

NOTE: Special ordering procedures have been established for Special Item Numbers (SINs) 132-51 IT Professional Services.

Orders placed pursuant to a Multiple Award Schedule (MAS), using the procedures in FAR 8.404, are considered to be issued pursuant to full and open competition. Therefore, when placing orders under Federal Supply Schedules, ordering offices need not seek further competition, synopsise the requirement, make a separate determination of fair and reasonable pricing, or consider small business set-asides in accordance with subpart 19.5. GSA has already determined the prices of items under schedule contracts to be fair and reasonable. By placing an order against a schedule using the procedures outlined below, the ordering office has concluded that the order represents the best value and results in the lowest overall cost alternative (considering price, special features, administrative costs, etc.) to meet the Government's needs.

- a. Orders placed at or below the micro-purchase threshold. Ordering offices can place orders at or below the micro-purchase threshold with any Federal Supply Schedule Contractor.
- b. Orders exceeding the micro-purchase threshold but not exceeding the maximum order threshold. Orders should be placed with the Schedule Contractor that can provide the supply or service that represents the best value. Before placing an order, ordering offices should consider reasonably available information about the supply or service offered under MAS contracts by using the "GSA Advantage!" online shopping service, or by reviewing the catalogs/pricelists of at least three Schedule Contractors and selecting the delivery and other options available under the schedule that meets the agency's needs. In selecting the supply or service representing the best value, the ordering office may consider:
 - (1) Special features of the supply or service that are required in effective program performance and that are not provided by a comparable supply or service;
 - (2) Trade-in considerations;
 - (3) Probable life of the item selected as compared with that of a comparable item;
 - (4) Warranty considerations;
 - (5) Maintenance availability;
 - (6) Past performance; and
 - (7) Environmental and energy efficiency considerations.
- c. Orders exceeding the maximum order threshold. Each schedule contract has an established maximum order threshold. This threshold represents the point where it is advantageous for the ordering office to seek a price reduction. In addition to following the procedures in paragraph b, above, and before placing an order that exceeds the maximum order threshold, ordering offices shall:

Review additional Schedule Contractors:

- (1) Catalogs/pricelists or use the "GSA Advantage!" online shopping service;
- (2) Based upon the initial evaluation, generally seek price reductions from the Schedule Contractor(s) appearing to provide the best value (considering price and other factors); and
- (3) After price reductions have been sought, place the order with the Schedule Contractor that provides the best value and results in the lowest overall cost alternative. If further price reductions are not offered, an order may still be placed, if the ordering office determines that it is appropriate.

NOTE: For orders exceeding the maximum order threshold, the Contractor may:

- (1) Offer a new lower price for this requirement (the Price Reductions clause is not applicable to orders placed over the maximum order in FAR 52.216-19 Order Limitations);
 - (2) Offer the lowest price available under the contract; or
 - (3) Decline the order (orders must be returned in accordance with FAR 52.216-19).
- d. Blanket Purchase Agreements (BPAs). The establishment of Federal Supply Schedule BPAs is permitted when following the ordering procedures in FAR 8.404. All schedule contracts contain BPA provisions. Ordering offices may use BPAs to establish accounts with Contractors to fill recurring requirements. BPAs should address the frequency of ordering and invoicing, discounts, and delivery locations and times.
 - e. Price reductions. In addition to the circumstances outlined in paragraph c. above, there may be instances when ordering offices will find it advantageous to request a price reduction. For example, when the ordering office finds a schedule supply or service elsewhere at a lower price or when a BPA is being established to fill recurring requirements, requesting a price reduction could be advantageous. The potential volume of orders under these agreements, regardless of the size of the individual order, may offer the ordering office the opportunity to secure greater discounts. Schedule Contractors are not required to pass on to all schedule users a price reduction extended only to an individual agency for a specific order.
 - f. Small business. For orders exceeding the micro-purchase threshold, ordering offices should give preference to the items of small business concerns when two or more items at the same delivered price will satisfy the requirement.
 - g. Documentation. Orders should be documented, at a minimum, by identifying the Contractor the item was purchased from, the item purchased, and the amount paid. If an agency requirement in excess of the micro-purchase threshold is defined so as to require a particular brand name, product, or feature of a product peculiar to one manufacturer, thereby precluding consideration of a product manufactured by another company, the ordering office shall include an explanation in the file as to why the particular brand name, product, or feature is essential to satisfy the agency's needs.

13. Federal Information Technology/Telecommunication Standards Requirements

Federal departments and agencies 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 offices, 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, D.C. 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, Maryland 20899, telephone number (301) 975-2833.

14. Security Requirements

In the event security requirements are necessary, the ordering activities may incorporate, in their delivery orders, a security clause in accordance with current laws, regulations, and individual agency policy; however, the burden of administering the security requirements shall be with the ordering agency. If any costs are incurred as a result of the inclusion of security requirements, such costs will not exceed ten percent (10%), or \$100,000, of the total dollar value of the order, whichever is less.

15. Contract Administration for Ordering Offices

Any ordering office, 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 Government's convenience, and (m) Termination for Cause (See C.1.).

16. GSA Advantage!

GSA Advantage! is an online, interactive electronic information and ordering system that provides online 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 (e.g., NetScape). The Internet address is <http://www.fss.gsa.gov/>.

17. Purchase of Open-Market, Non-Schedule Items

For administrative convenience, open-market (non-contract) items may be added to a Federal Supply Schedule Blanket Purchase Agreement (BPA) or an individual order, provided that the items are clearly labeled as such on the order, all applicable regulations have been followed, and price reasonableness has been determined by the ordering activity for the open-market (non-contract) items.

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; and
 - (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:

Upon request of the Contractor, the Government may provide the Contractor with logistics support, as available, in accordance with all applicable Government regulations. Such Government 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)

Federal Acquisition Regulation (FAR) 13.303-1(a) defines Blanket Purchase Agreements (BPAs) as "...a simplified method of filling anticipated repetitive needs for supplies or services by establishing 'charge accounts' with qualified sources of supply." The use of Blanket Purchase Agreements under the Federal Supply Schedule Program is authorized in accordance with FAR 13.303-2(c)(3), which reads, in part, as follows:

"BPAs may be established with Federal Supply Schedule Contractors, if not inconsistent with the terms of the applicable schedule contract."

Federal Supply Schedule contracts contain BPA provisions to enable schedule users to maximize their administrative and purchasing savings. This feature permits schedule users to set up "accounts" with Schedule Contractors to fill recurring requirements. These accounts establish a period for the BPA and generally address issues such as the frequency of ordering and invoicing, authorized callers, discounts, delivery locations, and times. Agencies may qualify for the best quantity/volume discounts available under the contract, based on the potential volume of business that may be generated through such an agreement, regardless of the size of the individual orders. In addition, agencies may be able to secure a discount higher than that available in the contract based on the aggregate volume of business possible under a BPA. Finally, Contractors may be open to a progressive type of discounting where the discount would increase once the sales accumulated under the BPA reach certain prescribed levels. Use of a BPA may be particularly useful with the new Maximum Order feature. See the Suggested Format, contained in this Schedule Pricelist, for customers to consider when using this purchasing tool.

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, Contractor's Reports of Sales and 552.238-76, Industrial Funding Fee, 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 receive 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 apply.

The requisitioning 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:

<http://www.luarline.com>

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

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

1. Scope

- a. The prices, terms, and conditions stated under Special Item Number 132-51 Information Technology Professional Services.
- b. The Contractor shall provide services at the Contractor's facility and/or at the Government location, as agreed to by the Contractor and the ordering office.

2. Performance Incentives

- a. When using a performance based statement of work, performance incentives may be agreed upon between the Contractor and the ordering office on individual fixed price orders or Blanket Purchase Agreements, for fixed price tasks, under this contract in accordance with this clause.
- b. The ordering office must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
- c. To the maximum extent practicable, ordering offices shall consider establishing incentives where performance is critical to the agency's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.
- d. The above procedures do not apply to Time and Material or labor hour orders.

3. Ordering Procedures for Services (Requiring a Statement of Work)

FAR 8.402 contemplates that GSA may occasionally find it necessary to establish special ordering procedures for individual Federal Supply Schedules or for some Special Item Numbers (SINs) within a Schedule. GSA has established special ordering procedures for services that require a Statement of Work. These special ordering procedures take precedence over the procedures in FAR 8.404 (b)(2) through (b)(3).

GSA has determined that the prices for services contained in the contractor's price list applicable to this Schedule are fair and reasonable. However, the ordering office using this contract is responsible for considering the level of effort and mix of labor proposed to perform a specific task being ordered and for making a determination that the total firm-fixed price or ceiling price is fair and reasonable.

(a) When ordering services, ordering offices shall:

(1) Prepare a Request (Request for Quote or other communication tool):

(i) A statement of work (a performance-based statement of work is preferred) that outlines, at a minimum, the work to be performed, location of work, period of performance, deliverable schedule, applicable standards, acceptance criteria, and any special requirements (i.e., security clearances, travel, special knowledge, etc.) should be prepared.

(ii) The request should include the statement of work and request the contractors to submit either a firm-fixed price or a ceiling price to provide the services outlined in the statement of work. A firm-fixed price order shall be requested, unless the ordering office makes a determination that it is not possible at the time of placing the order to estimate accurately the extent or duration of the work or to anticipate cost with any reasonable degree of confidence. When such a determination is made, a labor hour or time-and-materials proposal may be requested. The firm-fixed price shall be based on the rates in the schedule contract and shall consider the mix of labor categories and level of effort required to perform the services described in the statement of work. The firm-fixed price of the order should also include any travel costs or other incidental costs related to performance of the services ordered, unless the order provides for reimbursement of travel

costs at the rates provided in the Federal Travel or Joint Travel Regulations. A ceiling price must be established for labor-hour and time-and-materials orders.

(iii) The request may ask the contractors, if necessary or appropriate, to submit a project plan for performing the task, and information on the contractor's experience and/or past performance performing similar tasks.

(iv) The request shall notify the contractors what basis will be used for selecting the contractor to receive the order. The notice shall include the basis for determining whether the contractors are technically qualified, and provide an explanation regarding the intended use of any experience and/or past performance information in determining technical qualification of responses. If consideration will be limited to schedule contractors who are small business concerns as permitted by paragraph (2)(i) below, the request shall notify the contractors that will be the case.

(2) Transmit the Request to Contractors:

(i) Based upon an initial evaluation of catalogs and price lists, the ordering office should identify the contractors that appear to offer the best value (considering the scope of services offered, pricing, and other factors such as contractors' locations, as appropriate). When buying IT professional services under SIN 132-51 ONLY, the ordering office, at its discretion, may limit consideration to those schedule contractors that are small business concerns. This limitation is not applicable when buying supplies and/or services under other SINs as well as SIN 132-51. The limitation may only be used when at least three (3) small businesses that appear to offer services that will meet the agency's needs are available, if the order is estimated to exceed the micro-purchase threshold.

(ii) The request should be provided to three (3) contractors if the proposed order is estimated to exceed the micro-purchase threshold, but not exceed the maximum order threshold. For proposed orders exceeding the maximum order threshold, the request should be provided to additional contractors that offer services that will meet the agency's needs. Ordering offices should strive to minimize the contractors' costs associated with responding to requests for quotes for specific orders. Requests should be tailored to the minimum level necessary for adequate evaluation and selection for order placement. Oral presentations should be considered, when possible.

(3) Evaluate Responses and Select the Contractor to Receive the Order:

After responses have been evaluated against the factors identified in the request, the order should be placed with the schedule contractor that represents the best value. (See FAR 8.404.)

(b) The establishment of Federal Supply Schedule Blanket Purchase Agreements (BPAs) for recurring services is permitted when the procedures outlined herein are followed. All BPAs for services must define the services that may be ordered under the BPA, along with delivery or performance time frames, billing procedures, etc. The potential volume of orders under BPAs, regardless of the size of individual orders, may offer the ordering office the opportunity to secure volume discounts. When establishing BPAs, ordering offices shall:

(1) Inform contractors in the request (based on the agency's requirement) if a single BPA or multiple BPAs will be established, and indicate the basis that will be used for selecting the contractors to be awarded the BPAs.

(i) **SINGLE BPA:** Generally, a single BPA should be established when the ordering office can define the tasks to be ordered under the BPA and establish a firm-fixed price or ceiling price for individual tasks or services to be ordered. When this occurs, authorized users may place the order directly under the established BPA when the need for service arises. The schedule contractor that represents the best value should be awarded the BPA. (See FAR 8.404.)

(ii) **MULTIPLE BPAs:** When the ordering office determines multiple BPAs are needed to meet its requirements, the ordering office should determine which contractors can meet any technical qualifications before establishing the BPAs. When multiple BPAs are established, the authorized users must follow the

procedures in (a)(2)(ii) above, and then place the order with the Schedule contractor that represents the best value.

(2) Review BPAs Periodically: Such reviews shall be conducted at least annually. The purpose of the review is to determine whether the BPA still represents the best value. (See FAR 8.404.)

(c) The ordering office should give preference to small business concerns when two or more contractors can provide the services at the same firm-fixed price or ceiling price.

(d) When the ordering office's requirement involves products as well as executive, administrative, and/or professional services, the ordering office should total the prices for the products and the firm-fixed price for the services and select the contractor that represents the best value. (See FAR 8.404.)

The ordering office, at a minimum, should document orders by identifying the contractor from which the services were purchased, the services purchased, and the amount paid. If other than a firm-fixed price order is placed, such documentation should include the basis for the determination to use a labor-hour or time-and-materials order. For agency requirements in excess of the micro-purchase threshold, the order file should document the evaluation of Schedule contractors' quotes that formed the basis for the selection of the contractor that received the order and the rationale for any trade-offs made in making the selection.

Ordering procedures for other services available on schedule at fixed prices for specifically defined services or tasks should use the procedures in FAR 8.404. These procedures are listed in the pricelist, under "Information for Ordering Offices," paragraph #12.

4. 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 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.

5. Performance of Services

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

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

c. The Agency 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.

6. Inspection of Services

The Inspection of Services – Fixed Price (Aug. 1996) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection – Time-and-Materials and Labor-Hour (Jan. 1986) 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 Rights in Data – General, may apply.

8. Responsibilities of the Government

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

9. Independent Contractor

All 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 Government.

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 Government contract, without some restriction on 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 Government, ordering offices 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 services. Progress payments may be authorized by the ordering office 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 Government 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 (Alternate I (Apr. 1984)) at FAR 52.232-7 applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts (Feb. 1997) (Alternate II (Jan. 1986)) at FAR 52.232-7 applies to labor-hour orders placed under this contract.

13. Resumes

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

14. Open Market Costs

Open Market costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering agency 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 Services and Pricing

Labor pricing and descriptions can be found under SIN 132-51 section of this price proposal.

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

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act, (Agency) 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-4743G.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: the 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 Government that works better and costs less.

Signatures

_____	_____	_____	_____
Agency	Date	Contractor	Date

(CUSTOMER NAME)

BLANKET PURCHASE AGREEMENT

Pursuant to GSA Federal Supply Schedule Contract Number(s) GS-35F-4743G, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (Ordering Agency):

(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 Government 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.

Lunarline Professional Labor Category Descriptions

Commercial Job Title: Program Manager Minimum Technical Qualifications/Experience: Overall 8-10 years of experience in the IT industry, out of which at least five (5) years must be in the field of Project Management, Business Administration, Human Resources, and/or Client Relationship Management. Functional Responsibility: He/She is the central point of contact with the Contracting Officer, Contracting Officer's Representative and Task Managers. Is the senior manager responsible for coordinating the management of all work performed on this contract, including subcontractors, team members, and vendors. Keeps in constant touch with the project managers regarding the status of various task order projects, the issues facing the project teams and effectively and regularly updates the client representatives. Also facilitates the information, which the team requires from the client to effectively implement various Task Order Projects and if necessary, escalates the burning issues to the client representatives and contract officer. All the Task Order Project Managers typically report to the Program Manager for that contract. Minimum Education: Bachelor's degree or equivalent technical qualification or 2-3 years of additional experience. Master's Degree in Computer Science; Master's Degree in Business Administration is desirable.

Commercial Job Title: Project Manager Minimum Technical Qualifications/Experience: At least five (5) years experience in managing Information Technology projects. Must have a thorough knowhow of Software Development Lifecycle, project planning, risk management, project reporting, proficiency in Project Management tools like MS Project, tools like Visio, MS Word, Excel and Power Point. Functional Responsibility: The Project manager is responsible for the timely execution of the various Task Order projects awarded under the master contract. He/She is responsible for project planning, team composition, task allocation, task monitoring, task facilitation, risk management, disaster recovery, over viewing analysis/designing, programming, testing and technical and user documentation, maintaining project status documentation, giving regular updates to the Account manager, giving technical presentations to the client representatives and periodically attend status meetings with the client representatives. Reports to the Program Manager for the contract. Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Master's Degree in Computer Science a big plus. Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have at least seven years of experience in managing IT projects.

Commercial Job Title: System/Software Architect Minimum Technical Qualifications/Experience: Eight (8) years of experience in the field of Information Technology out of which at least five years must be devoted to designing various components of Information systems for organizations based on the various business processes and applications. Must be very familiar with design tools like ERWin, Visio and Rational Rose and must have architected at least 3 systems in the past. Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with the company's business and technology direction and objectives. Also, designs and develops new software products or major enhancements to existing software. Addresses problems of systems integration, compatibility, and multiple platforms. Develops information technology technical and application architectures and participates in setting technology direction and standards. Provides technical architectural design review for major business applications and technology initiatives. Facilitates linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develops recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually reviews the company's applications, workflow, systems, and network management and network infrastructure, for opportunities to improve effectiveness and efficiency. Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or

Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast ten years of experience in architecturing IT systems.

Commercial Job Title: Configuration Management Specialist Minimum Technical

Qualifications/Experience: Three to Five years of general IT experience, with three (3) years of specialized experience in Configuration Management, Version Control, Process Improvement, Activity/Process Modeling. Must be familiar with one or more of the Configuration Tools like Clearcase, PVCS, Endeavor, CMVC and Visual SourceSafe

Functional Responsibility: Supports the development and maintenance of configuration management plans, and scheduling and documenting configuration management reviews. Shall be capable of monitoring the configuration control process and ensuring that procedures comply with client and/or applicable specifications. Reports to Lead Configuration Management Specialist and requires supervision.

Knowledgeable of software development techniques, change control processes, configuration audits and client/government regulations, manuals, technical orders, standards and industry publications related to configuration/data management required to perform the task. Requires supervision.

Educational Requirement: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast five years of experience in performing Configuration Management and Version Control Tasks.

Commercial Job Title: Technical Instruction Specialist

Minimum/General Experience: Experience should include at 5 - 7 years of managing Technology and Security training programs including training documentation. Experience with multimedia aided instruction is preferred.

Functional Responsibility: Provides computer training and classroom instructions to users and staff personnel as appropriate. Gathers and assemble relevant material to be presented. Utilize appropriate teaching methods, individual, group, workshops, etc. Ensure students understand the theoretical and practical aspects of subject material/software application/database applications being taught. Evaluates effectiveness of instruction by ensuring students have a thorough knowledge of subject matter and hands-on skill at performing required task.

Educational Requirement: Bachelor's degree or equivalent technical qualification or 2-3 years of additional experience. Minimum one (1) year of training development and delivery experience.

Commercial Job Title: Information Assurance Engineer Minimum Technical Qualifications/Experience:

Overall four years of experience in defining IS

Security policies, analyzing, designing,, implementing, integrating and maintaining the Information Security of firms.

Functional Responsibility: Analyzes and defines security requirement for computer systems which may include mainframes, workstations, and personal computers. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution. Establishes and satisfies complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Supports customers at the highest levels in the development and implementation of doctrine and policies. Applies know-how to government and commercial common user systems, as well as to dedicated special purpose systems requiring specialized security features and procedures.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast six years of experience in

analyzing, designing,, implementing, integrating and maintaining the Information Security of firms.

Commercial Job Title: Information Security Analyst Minimum Technical Qualifications/Experience:

Overall five years of experience in analyzing

computer security at large firms, conducting gap analysis, identifying and alleviating potential loopholes.

Functional Responsibility: Analyzes the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures.

Ensures that all information systems are functional and secure.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast seven years of experience in analyzing computer security at large firms.

Commercial Job Title: Information Assurance System/Network Specialist Minimum Technical

Qualifications/Experience: Overall five years of experience in installing, configuring, and maintaining

organization's operating systems, and network components to

ensure security of networks.

Functional Responsibility: Installs, configures and maintains organization's operating systems. Analyzes and resolves problems associated with server hardware, NT, applications software. Detects, diagnoses, and reports NT related problems on both NT server and NT desktop systems. Performs a wide variety of tasks in software/hardware maintenance and operational support of NT Server systems. Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast seven years of relevant experience in installing, configuring, and maintaining organization's operating systems, and network components.

Commercial Job Title: Senior Information Security Specialist Minimum Technical

Qualifications/Experience: Overall eight years of experience in defining,

implementing and maintaining the Information Security of firms. Must have strong know-how of Encryption, Intrusion Detection, Network Security and Ethical Hacking.

Functional Responsibility: Responsible for defining/ameliorating the IS Policy, including Disaster Recovery Policy for client organizations. Also responsible for ensuring that the organization networks as well as information is secure at all times by constantly monitoring intrusion detection, data encryption, and taking quick and effective corrective measures in the event of a breach. Provides technical knowledge and analysis of information assurance, to include applications; operating systems; Internet and Intranet; physical security; networks; risk assessment; critical infrastructure continuity and contingency planning; emergency preparedness; security awareness and training. Provides analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provides technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Provides system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintains servers, creates monitoring reports and logs and ensures functionality of links.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other

than those listed above will also be considered if and only if they have atleast 10 years of experience in defining, implementing and maintaining the Information Security of firms.

Commercial Job Title: IT Subject Matter Expert Minimum Technical Qualifications/Experience: Five to seven years of experience in studying, analyzing, evaluating, designing and improving specific programs and business processes (example: expertise in Naval Air Defense Systems, Child Support Programs, Teachers Licensing Programs, CFR validation, Treasury Systems, Driver Licensing Systems, Housing Loan Programs or any other program critical to designing/improving the Information Systems), help define the Software Requirement Specifications and Business Process Documents and assist the System Architect in architecturing the system.

Functional Responsibility: Responsible for serving as facilitator for Integrated Product Team, defining/ameliorating the policies and procedures of an organization, process or program. Utilizing their specialization and subject matter knowhow to assist the business analysts and Project Managers in defining the Software Requirement Specifications and Business Process Documents and assist the System Architect in architecturing the system. Also assist the testing team in Integrated System testing to ensure that the system is working under various conditions/scenarios critical for the program or the application.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast nine years of experience working with the functional and technical aspects of various programs like Naval Air Defense Systems, Child Support Programs, Teachers Licensing Programs, CFR validation, Treasury Systems, Driver Licensing Systems, Housing Loan Programs or any other program critical to designing/improving the Information Systems

Commercial Job Title: Applications Developer Minimum Technical Qualifications/Experience: Overall three to five years of experience in independently developing and testing various mission critical applications and implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi- programming technology, database management techniques, and data communications protocol. Must be skilled in programming in the relevant programming language/s (Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix Shell scripting)

Functional Responsibility: Performs the development and/or programming, and implementation of information processing systems and applications that use current operating systems, programming languages and applications development tools, computer systems, multi- programming technology, database management techniques, and data communications protocol. Can work independently in support of a joint applications development effort. Responsible for writing application software, data manipulation, databases programming, testing and implementation, technical and user documentation, software conversions; environments include but are not limited to mainframe, mid range, personal computers, laptops.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast six years of experience in independently developing industry applications.

Commercial Job Title: Senior Applications Developer Minimum Technical Qualifications/Experience: Overall six to eight years of experience in supervising and mentoring other Application developers in the performance of detailed analysis, in building software development tools and in producing highly technical programs such as cross-compilers and communications software operating systems. Must be proficient in programming in the relevant programming language/s (Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix

Shell scripting)

Functional Responsibility: Directs the activities of other programmers and analysts in the performance of detailed analysis, in building software development tools and in producing highly technical programs such as cross-compilers and communications software operating systems. Responsible for measuring software performance through project design, implementation and evaluation of results. Supervises and participates in the development of manuals and user guides for programmers and operating staff. Establishes and supervises the design of software necessary to integrate new hardware and codes programs in applicable languages using detailed flow diagrams and input/output descriptions as guidelines. Supervises software analysis, the development of program specifications and the development of program code. Performs implementation tasks and directs the conduct of application testing to insure results. Directs and participates in the development of manuals and user guides for programmers and operating staff.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast ten years of experience in supervising and mentoring other Application developers in the performance of detailed analysis, in building software development tools and in producing highly technical programs such as cross-compilers and communications software operating systems.

Commercial Job Title: Analyst (Business/System/Data)

Minimum Technical Qualifications/Experience: Overall six (6) years of experience in analyzing the business processes, data and Information Systems of organizations, mentoring other Business/System Analysts, coordinating and supporting the development, enhancement, and maintenance of products and services applicable to multiple lines of a customer's business using information technology

Functional Responsibility: Coordinates and supports the development, enhancement, and maintenance of products and services applicable to multiple lines of a customer's business using information technology. Also responsible for technically analyzing the business processes, data and/or Information Systems of organizations. This includes the analysis of the architecture of the system, what hardware, operating system and software the organization uses, what is the role of each hardware and software element, what databases the organization runs and on what platforms, is the data being used reliable, which processes run on which platform/hardware, in what programming languages have the business logic been written. Anticipates and identifies user problems and needs. Recommends business solutions based on customer requirements and industry trends. Leads, plans, schedules, and controls complex projects and activities with customers, support groups, and vendors on concurrent projects. Applies extensive knowledge of the customer's business and industry to develop project specifications. Advises on methods to improve business processes and remove non-value added activities. Coordinates and participates in proposals, feasibility studies, implementations, and new business development. leads the training of customers and peers and builds relationships with multiple customer levels.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if and only if they have atleast eight years of experience in analyzing the business processes and Information Systems of organizations.

Commercial Job Title: Application Integration Specialist **Minimum Technical Qualifications/Experience:** Overall 6-8 years of technical experience with the integration of multi-vendor software and hardware components in Client/Server, LAN and WAN environments. Requires competence in software and hardware implementation, analysis techniques, concepts and methods. Proven ability to work well independently and with minimum supervision.

Functional Responsibility: Provides computer systems expertise on projects requiring establishment of a new automated information system where integration with existing systems is required. Performs systems

analysis, development of alternative solutions, and design of technical and business solutions. Working with minimal supervision, conducts project feasibility and implementation studies, including the development of plans and testing for evaluation. Develops and implements data conversion routines. Performs system testing to insure satisfactory results. Duties require knowledge of data sources, data flow, system interactions, and computer equipment and software applications. May perform selected project tasks independently or with minimal direction. Provides technical support to the project team.

Establishes and maintains development, testing environments and the configuration management process and structures. Serves as point-of-contact for third-party software and hardware vendors.

Minimum Education: Bachelors Degree in Computer Science, Information Systems, Engineering, Business, Economics, Mathematics or Public Administration. Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have at least ten years of experience with the integration of multi-vendor software and hardware components in Client/Server, LAN and WAN environments, software and hardware implementation, analysis techniques, concepts and methods.

Commercial Job Title: Quality Assurance Specialist Minimum Technical Qualifications/Experience:

Overall Eight (8) years of experience in defining

test cases, developing test plans and leading the software testing and validation teams in performing the unit, and integrated system (functional, load, regression) testing of complex software/systems. Must have a thorough understanding of Software Testing and Quality Assurance Methodologies like IEEE, SEI CMM/I, ISO 9000, and TQA.

Functional Responsibility: Provides development of project Software Quality Assurance Plan and the implementation of procedures that conforms to the requirements of the contract as detailed in Quality Assurance Surveillance Plan. Provides an independent assessment of how the project's software development process is being implemented relative to the defined process and recommends methods to optimize the organization's process. Performs regular internal audits to ensure proper quality control. The QA Specialist is responsible for system and/or application testing (client server and web applications) to ensure that the system/application software is compliant with the access control exposure. Detailed tasks include developing a system/application test plan/design, test procedures and complete test reporting documentation, test execution and tracking, and release management. Includes testing both the functionality of the application via the front end and validate the test results vial the back-end. Testing is done using several testing tools like Load runner and WinRunner. Responsible for developing the test cases system/application test plan/design, test procedures and leading a team of testers in performing the unit, and integrated system (functional, load, regression) testing of complex software/systems. Responsible for reviewing the test reporting documentation, test execution and tracking, and release management. Responsible for ensuring that the system/application software is compliant with the access control exposure.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, Economics, Mathematics or Public Administration.

Commercial Job Title: Software Tester Minimum Technical Qualifications/Experience: Overall five (5) years of experience in independently performing unit and system integration testing (load, functional and regression testing) manually as well as using automated tools like Load Runner, WinRunner and Test Director. Must have expertise in both black box as well as white box testing. Must know how to conduct application, regression and load testing.

Functional Responsibility: Responsible for performing the system and/or application testing (client server and web applications) to ensure that the system/application software is compliant with the access control exposure. Responsible for following the test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify bugs and the root cause.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, Economics, Mathematics or Public Administration. Candidates having Bachelors Degree in disciplines other

than those listed above will also be considered if they have at least seven years of experience in performing unit and integration testing manually as well as using automated tools like Load Runner, WinRunner and Test Director.

Commercial Job Title: Internet Developer Minimum Technical Qualifications/Experience: Overall four (4) years of experience in

independently analyzing web systems and developing Internet/Intranet applications in .Net, XML, Java, EJB and Java Script and deploying the applications on the Application Servers like Weblogic, Websphere and iPlanet. Must be proficient in one or more of .Net, Java, HTML, DHTML, JavaScript, CGI, Cold Fusion, COM/DCOM, CORBA.

Functional Responsibility: Analyzing, understanding the architecture and developing Internet applications using languages like Microsoft .Net, Java, XML, JSP, EJB and Javascript and deploying the applications on the Application Servers like Weblogic, Websphere and iPlanet. Also responsible for writing interfaces, developing stored Procedures, Triggers and Views, Unit testing and code review. Can work independently in support of a joint applications development effort.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have at least six years of experience in independently developing industry Internet/web applications.

Commercial Job Title: Senior Internet Developer Minimum Technical Qualifications/Experience: Overall eight (8) years of experience in leading

the analyzing systems and developing and Internet/Intranet applications in .Net, XML, Java, EJB and Java Script and deploying the applications on the Application Servers like Weblogic, Websphere and iPlanet.

Must be proficient with Web Architecture and Development Methodologies

Functional Responsibility: Lead a team of Internet Developers in Analyzing, designing, developing and testing Internet applications using languages like Microsoft .Net, Java, XML, JSP, EJB and Javascript and deploying the applications on the Application Servers like Weblogic, Websphere and iPlanet. Responsible for unit testing, code review, preparing technical and user documentation.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical).

Commercial Job Title: Database Designer Minimum Technical Qualifications/Experience: Overall five years experience in analyzing and designing databases (Oracle, MS SQL, DB2, DMS, Sybase).

Functional Responsibility: Responsible for designing the database. This includes the design of the tables, fields, screens, triggers and stored procedures so as to optimize the database performance (efficiency, reliability, scalability). Will analyze database systems and programs, which include access methods, access time, file structures, device allocation, validation checks, statistical methods, and security. Will also work with user community to understand data access and integration needs, ensure integration of systems through the database structure, perform data modeling, monitor database standards and procedures, system usage and performance, troubleshoot and resolve database and data problems, and develop and administer disaster recovery plans.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have at least seven years of experience analyzing and designing databases.

Commercial Job Title: Database Administrator Minimum Technical Qualifications/Experience: Five (5) years general experience including two (2) years specialized experience. Requires some supervisory

responsibility and management interface. Two of the four years of experience must include providing direction to personnel performing database administration tasks and technical expertise in using at least one of the following DBMS products relevant to the specific task: IMS, DB2, ADABAS, ORACLE, SYBASE, SQL Server, INGRES.

Functional Responsibility: Responsible for

- Installing the database on the server as well as installing the clients.
- Maintaining and creating Users, Nodes, Instances, Databases, Tables Spaces,
- Containers, Buffer Pools and Logs.
- Migrating data between databases.
- Extracting data from one system into flat files and then loading into the database
- without constraints.
- Writing Stored procedures, Triggers to populate data from non-constraints tables to
- normalized tables with constraints.
- Tuning the database manager configuration, database configuration parameters like
- Bufferpools, Shared Memory variables, I/O variables, Application heap, Database
- heap size, Logs and Sort area to increase performance of the system.
- Analyzing the execution path of the query to determine the cost, indexing and cardinality.
- Writing scripts to create instances, databases, scheduling online, offline backups and restoring databases.
- Implementing Active- Standby Clustering, database partitioning using utilities.

Also, provides highly technical expertise and guidance in the design, implementation, operation and maintenance of database management systems (DBMS). Evaluates and recommends available DBMS products after matching requirements with system capabilities. Determines file organization, indexing methods, and security procedures for specific applications. Controls the design and use of databases. Controls the global view of databases, controls the access to the databases, assures the safekeeping of the databases (from accidental or intentional damage or loss), and monitors the use of databases. Must be capable of defining all required database administration policies, procedures, standards, and guidelines. Is an authority on the design of databases and the use of database management systems. Evaluates and recommends available DBMS products after matching requirements with system capabilities. Prepares and delivers presentations on DBMS concepts.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have atleast seven years of experience in database administration.

Commercial Job Title: aSystemAdministrator Minimum Technical Qualifications/Experience: Overall five years of experience in installing, managing, maintaining and troubleshooting hardware and software on

systems (Windows, HP Unix, Sun Solaris, MVS, VMM Unisys 2200) on different platforms like mainframe, midrange and PCs. Must also have

Functional Responsibility: Responsible for the installing, managing, maintaining and troubleshooting hardware and software on systems, to maintain the on-going operational performance of programs (software) and the hardware on which the programs run within the Mainframe, Mid-Range, or PC environments. Implements and supports local area network (LAN) and campus area network (CAN) hardware and software. Analyzes customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Acts as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyzes performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implements operational support standards and procedures relating to change management, performance management, and security. Recommends changes and improvements to existing standards. Develops site administration manual (SAM) documentation. Provides user orientation on hardware, software and network operations.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have atleast seven years of experience in installing, managing, maintaining and troubleshooting hardware and software on systems (Windows, HP Unix, Sun Solaris, MVS, VMM Unisys 2200) on different platforms like mainframe, midrange and PCs.

Commercial Job Title: Network Engineer **Minimum Technical Qualifications/Experience:** Overall four (4) years of experience in networking administration. Must be knowledgeable in computer technology, including architecture, operating systems, and hardware components, such as workstations, disks, and graphics input and output devices; must be knowledgeable in distributed computing system concepts, including client/server computing issues, mass storage technology, and computer network technology. Must have experience in configuring UNIX workstations, including SunOS and SPARC products, and associated third party peripherals. Mass storage experience should include optical technology; must thoroughly understand complex network principles related to IEEE802, ISDN, X.25, TI, TCP/IP, and NFS. This should include protocol specifications, performance limitations, network inter-connectivity issues, and network security. Network experience must include configuring one or more networks based on serial communications, MODEMS, Ethernet, TCP/IP, and NFS. It is desirable to have UNIX software development experience; must have ability to effectively communicate technical information to non-technical personnel, both orally and in writing.

Functional Responsibility: Responsible for developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms. Designs, develops, tests and implements new system software modules and enhancements to current systems; designs, develops, tests, and implements diagnostic utilities to analyze and report system status and performance. Monitors and evaluates overall system performance of operating system facilities, software products, computer services, and communications and networking facilities; specifies, installs and tests system components as required to enable system to meet desired performance objectives.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have atleast seven years of experience in developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms

Commercial Job Title: Senior Network Engineer **Minimum Technical Qualifications/Experience:** Overall six (6) years of experience in planning, management, support, and operation of the LAN/WAN environment. Must be knowledgeable in computer technology, including architecture, operating systems, and hardware components, such as workstations, disks, and graphics input and output devices; must be knowledgeable in

distributed computing system concepts, including client/server computing issues, mass storage technology, and computer network technology. Must have experience in configuring UNIX workstations, including SunOS and SPARC products, and associated third party peripherals. Must thoroughly understand complex network principles related to IEEE802, ISDN, X.25, TI, TCP/IP, and NFS. This should include protocol specifications, performance limitations, network inter-connectivity issues, and network security. Network experience must include configuring one or more networks based on serial communications, MODEMS, Ethernet, TCP/IP, and NFS. It is desirable to have UNIX software development experience; must have ability to effectively communicate technical information to non-technical personnel, both orally and in writing.

Functional Responsibility: Responsible for planning, management, support, and operation of the LAN/WAN environment. Provides system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintains servers, creates monitoring reports and logs and ensures functionality of links. Establishes backups and monitors site security. Responsible for developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms. Designs, develops, tests and implements new system software modules and enhancements to current systems; designs, develops, tests, and implements diagnostic utilities to analyze and report system status and performance. Evaluates overall system performance of operating system facilities, software products, computer services, and communications and networking facilities; specifies, system components as required to enable system to meet desired performance objectives.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical). Candidates having Bachelors Degree in disciplines other than those listed above will also be considered if they have at least eight years of experience in planning, management, support, and operation of the LAN/WAN environment.

Commercial Job Title: E-Government Specialist Minimum Technical Qualifications/Experience: Five (5) years of experience in conceptualizing, analyzing, designing and implementing the web modules, web based applications and web sites for State and/or Federal Government.

Functional Responsibility: Responsible for need analysis, conceptualization, analysis, design and implementation of web applications, web modules, e-forms, web sites and portals for the State and Federal Government agencies. Responsible for improvements to the existing Government Web applications.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Business, Arts, Economics, Mathematics or Engineering (Electrical, Computer, Mechanical).

Labor Category	Government / Contractor Site Year 1 Hourly Rate
	\$/hr
Program Manager	134.20
Project Manager	134.20
System/Software Architect	129.37
Configuration Management Specialist	85.92
Technical Instruction Specialist	85.92
Information Assurance Engineer	124.54
Information Security Analyst	128.40
Information Assurance System/Network Specialist	134.20
Senior Information Security Specialist	143.84
IT Subject Matter Expert	138.06
Application Developer	89.78
Senior Application Developer	112.96
Analyst (Business/System/Data)	124.54
Application Integration Specialist	134.20
Quality Assurance Specialist	124.54
Software Tester	89.78
Internet Developer	93.65
Senior Internet Developer	118.75
Database Designer	124.54
Database Administrator	128.40
System Administrator	128.40
Network Engineer	93.65
Senior Network Engineer	128.40
E-Government Specialist	134.20
Junior Information Security Analyst	50.05
Junior Technical Writer	55.06
InfoSec Engineer	66.43
Application Analyst	68.25
Junior Information Assurance Engineer	70.98
Penetration Tester	72.80
Certification Specialist	75.53
Mid-Level Information Assurance Engineer	77.35
Computer System Security Specialist	83.35
Junior Enterprise Architect	93.73
IT Technologist	95.55
Enterprise Architect - Mid	109.20
Project Control Analyst	132.74
R&D Specialist	142.39
Security Subject Matter Expert	142.39
Information System Security Specialist	147.94
Help Desk Analyst	47.32

Lunarline Training Course Descriptions

DIACAP IN-DEPTH WORKSHOP 5 DAY

DoD Information Assurance Certification and Accreditation Process

OVERVIEW:

This course provides an in-depth look into the DIACAP process and hands-on training of developing the DIACAP Systems Identification Profile (SIP), DIACAP Implementation Plan (DIP), and Plan of Actions and Milestones (POA&M). This course also reviews DoD IA tools, the DISA Connection Approval Process (CAP), and information related to the C&A Transformation.

Every student participating in the DIACAP Hands-On In-Depth 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

MODULES:

1. C&A Overview and DoD Information Assurance Policy
2. DoD's Current IA Policy Framework
3. DoD Information Systems
4. DITSCAP to DIACAP
5. DIACAP Overview
6. In-depth DIACAP Activity Cycle: Activity 1 – Initiate and Plan
7. In-Depth DIACAP Activity Cycle: Activity 2- Implement & Validate IA Controls
8. In-Depth DIACAP Activity Cycle: Activity 3 – Certification Determination & Accreditation Decision
9. In-Depth DIACAP Activity Cycle: Activity 4 – Maintain ATO & Conduct Annual Reviews (Situational Awareness)
10. In Depth DIACAP Activity Cycle: Activity 5 – System Decommission
11. Applying the DIACAP to the System Lifecycle
12. Overview of IA Tools
13. The Principle of Reciprocity
14. Future of C&A – Moving the DIACAP to a Risk Management Framework
15. CAPSTONE Exercise

Lunarline's DIACAP Training Classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) – DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

DIACAP VALIDATOR WORKSHOP 5 Day

DoD Information Assurance Certification and Accreditation Process

OVERVIEW:

This course concentrates on methods used to validate DoD IA Controls as contained in DoDI 8500.2. Discussion areas include an overview of the DIACAP, the DoD-defined information system types and the associated security concerns, vulnerability scanning, DoD-approved automated scanning tools, and many more. The course provides an in-depth explanation of each control identified in DoDI 8500.2 to include the appropriate testing method, associated supporting evidence (known as artifacts), and how to more efficiently and effectively test and validate DoD systems and infrastructure. The curriculum will prepare the ACA or

Validator to test against the DoD IA controls using manual and automated procedures in accordance with the standards set forth by the Department.

MODULES:

1. Introduction
2. Critical Definitions
3. DoD's Current IA Policy Framework
4. Overview of the DIACAP
5. DIACAP Activity Cycle
6. DIACAP Validation Tests
7. Validator Toolkit
8. The Future of C&A
9. CAPSTONE

Lunarline's DIACAP Training Classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) – DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the DIACAP Validator Workshop 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

DIACAP HANDS-ON INTENSITY 4 DAY

DoD Information Assurance Certification and Accreditation Process

OVERVIEW:

This course is designed for students who want to gain an improved understanding of the DIACAP. The course provides an overview of DIACAP requirements, documentation, and associated processes. The 4-day intensity course provides an in-depth look into the DIACAP processes, and includes a series of hands-on exercises in developing the DIACAP Systems Identification Profile (SIP), DIACAP Implementation Plan (DIP), and Plan of Actions and Milestones (POA&M). The DIACAP training is introduced from a Department perspective, but can be tailored as required to include Component/Service and system-specific nuances relative to the implementation of the DIACAP. Instruction modules include the DIACAP Activity Cycle, the Knowledge Service, DIACAP Governance Structure, roles and responsibilities, and many more. The fourth day of the DIACAP Intensity course provides each student with an introduction to using the DoD approved automated scanning tools, including the DISA SRRs, Gold Disk, and other DoD automated tools.

MODULES:

1. C&A Overview and DoD Information Assurance Policy
2. DoD's Current IA Policy Framework
3. DoD Information Systems
4. DITSCAP to DIACAP
5. DIACAP Overview
6. DIACAP Activity Cycle: Activity 1 – Initiate and Plan
7. DIACAP Activity Cycle: Activity 2- Implement & Validate IA Controls
8. DIACAP Activity Cycle: Activity 3 – Certification Determination & Accreditation Decision
9. DIACAP Activity Cycle: Activity 4 – Maintain ATO & Conduct Annual Reviews (Situational Awareness)

10. DIACAP Activity Cycle: Activity 5 – System Decommission
11. DIACAP and the System Lifecycle
12. DIACAP supporting Tools
13. Future of C&A
14. Certification Testing

Lunarline’s DIACAP Training Classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) – DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-authored by Lunarline’s VP of Cybersecurity and CEO.

Every student participating in the DIACAP Hands-On Intensity 4 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

DIACAP Hands-On In-Depth 3 Day

DoD Information Assurance Certification and Accreditation Process

OVERVIEW:

This course is designed for students who want to gain an improved understanding of the DIACAP. The course provides an overview of DIACAP requirements, documentation, and associated processes. This course provides an in-depth look into the DIACAP processes, and includes a series of hands-on exercises in developing the DIACAP Systems Identification Profile (SIP), DIACAP Implementation Plan (DIP), and Plan of Actions and Milestones (POA&M). The DIACAP training is introduced from a Department perspective, but can be tailored as required to include any Component/Service or system-specific nuances relative to the implementation of the DIACAP. Instruction modules include the DIACAP Activity Cycle, the Knowledge Service, DIACAP Governance Structure, roles and responsibilities, and much more.

MODULES:

1. C&A Overview and DoD Information Assurance Policy
2. DoD’s Current IA Policy Framework
3. DoD Information Systems
4. DITSCAP to DIACAP
5. DIACAP Overview
6. DIACAP Activity Cycle: Activity 1 – Initiate and Plan
7. DIACAP Activity Cycle: Activity 2- Implement & Validate IA Controls
8. DIACAP Activity Cycle: Activity 3 – Certification Determination & Accreditation Decision
9. DIACAP Activity Cycle: Activity 4 – Maintain ATO & Conduct Annual Reviews (Situational Awareness)
10. DIACAP Activity Cycle: Activity 5 – System Decommission
11. DIACAP and the System Lifecycle
12. DIACAP supporting Tools
13. Future of C&A
14. Certification Testing

Lunarline’s DIACAP Training Classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) – DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-

authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the DIACAP Hands-On In-Depth 3 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

DIACAP Hands-On Overview 1 Day

DoD Information Assurance Certification and Accreditation Process

OVERVIEW:

This course is designed for students who want to gain an improved understanding of the DIACAP. The course provides an overview of DIACAP requirements, documentation, and associated processes.

Lunarline's DIACAP Training Classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) – DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Applying the FISMA/NIST Risk Management Framework / 800-53 Security Controls

Validator 5 Day

Federal Information Security Management Act

OVERVIEW:

Every student participating in Lunarline's FISMA/NIST Validator 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

This course provides an in-depth look at testing the controls using NIST SP 800-53A and ensuring the use of the Risk Management Framework (RMF) for Federal Security Systems.. The focus of the course is an in-depth explanation of each NIST SP 800-53 Revision 3 controls to include what method should be used to test and validate each security control in accordance with NIST SP 800-53A and NIST SP 800-115, what evidence should be gathered, and how to more efficiently and effectively test Federal systems and infrastructure. The curriculum will introduce the independent tester or Validator to test the process for any of the Federal IA controls using manual and automated tests to ensure all controls are tested properly.

The FISMA Validator Course will cover NIST SP 800-53A, NIST SP 800-115, NIST SP 800-37, NIST SP 800-39 and the development of the Security Assessment Report (SAR), and Plan Of Action and Milestones (POA&M). The student will have a hands-on experience using scenario- based hands-on exercises in executing the validation tests with the approved tools. These exercises will include the development of the Security Assessment Report (SAR).

Lunarline's courseware has been evaluated and is the only industry training certified by the NSA/CNSS to meet NSTISSI No. 4011 and 4015 requirements. All of our instructors have hands-on, real world experience – you get more than just classroom instruction, you receive the benefits of actual expertise in executing these processes.

This course includes the following takeaway items: A printed training manual, a CD with a comprehensive set of NIST and Director of National Intelligence (DNI) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the Applying the FISMA/NIST Risk Management Framework / 800-53

Security Controls Validator 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

Applying the FISMA/NIST Risk Management Framework In-Depth 3 Day

Federal Information Security Management Act

OVERVIEW:

Lunarline's Federal Information Security Management Act (FISMA) training provides students with a fundamental knowledge of the requirements for meeting FISMA requirements, as well as an in-depth look of the Federal system authorization process and Risk Management Framework (RMF). This training equips the students with an in-depth indoctrination into the RMF and they will learn the requirements for managing risk, and ensuring that the confidentiality, availability and integrity of federal information and information systems is protected at a level commensurate with the security requirements of the information and the information system. Students will participate in a series of scenario-based hands-on exercises to enhance understanding of the processes used for system authorization, including all of the elements of the Risk Management Framework. These exercises will include the development of Systems Security Plans (SSPs), Security Assessment Reports (SARs), and Plans Of Action and Milestones (POA&Ms) for Federal Information Systems. This training is a CNSS approved course that deals with the new C&A transformation. Please note – this course has been aligned with NIST SP 800-37 Revision 1 and is the new process under the C&A transformation.

The FISMA In-Depth Course covers the requirements and the use of FIPS 199, NIST SP 800-60, NIST SP 800-37 Revision 1, NIST SP 800-39, NIST SP 800-30, NIST SP 800-34, NIST SP 800- 53 Revision 3, and NIST SP 80053A.

MODULES:

1. Critical Definitions and Policies
2. C&A Transformation/Transition Overview
3. The IC and the Transformation
4. Roles and Responsibilities
5. Accreditation Boundary
6. System Categorization
7. Select Security Controls
8. Implement, Document & Assess Security Controls
9. Authorize Information System
10. Monitor Information System
11. Reciprocity

Lunarline's FISMA/NIST classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of NIST and Director of National Intelligence (DNI) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the Apply the FISMA/NIST Risk Management Framework In- Depth 3 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

Applying the FISMA/NIST Risk Management Framework In-Depth 3 Day

Federal Information Security Management Act

OVERVIEW:

Lunarline’s Federal Information Security Management Act (FISMA) training provides students with a fundamental knowledge of the requirements for meeting FISMA requirements, as well as an in-depth look of the Federal system authorization process and Risk Management Framework (RMF). This training equips the students with an in-depth indoctrination into the RMF and they will learn the requirements for managing risk, and ensuring that the confidentiality, availability and integrity of federal information and information systems is protected at a level commensurate with the security requirements of the information and the information system. Students will participate in a series of scenario-based hands-on exercises to enhance understanding of the processes used for system authorization, including all of the elements of the Risk Management Framework. These exercises will include the development of Systems Security Plans (SSPs), Security Assessment Reports (SARs), and Plans Of Action and Milestones (POA&Ms) for Federal Information Systems. This training is a CNSS approved course that deals with the new C&A transformation. Please note – this course has been aligned with NIST SP 800-37 Revision 1 and is the new process under the C&A transformation.

The FISMA In-Depth Course covers the requirements and the use of FIPS 199, NIST SP 800-60, NIST SP 800-37 Revision 1, NIST SP 800-39, NIST SP 800-30, NIST SP 800-34, NIST SP 800- 53 Revision 3, and NIST SP 80053A.

MODULES:

1. Critical Definitions and Policies
2. C&A Transformation/Transition Overview
3. The IC and the Transformation
4. Roles and Responsibilities
5. Accreditation Boundary
6. System Categorization
7. Select Security Controls
8. Implement, Document & Assess Security Controls
9. Authorize Information System
10. Monitor Information System
11. Reciprocity

Lunarline’s FISMA/NIST classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of NIST and Director of National Intelligence (DNI) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-authored by Lunarline’s VP of Cybersecurity and CEO.

Every student participating in the Apply the FISMA/NIST Risk Management Framework In- Depth 3 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

Applying the CNSS/NIST Risk Management Framework / 800-53 Security Controls

Validator 5 Day

Certified Committee on National Security Systems

OVERVIEW:

Every student participating in Lunarline’s CNSS/NIST Validator 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

This course provides an in-depth look at testing the controls using NIST SP 800-53A, CNSS 1253A, and

ensuring the use of the Risk Management Framework (RMF) for National Security Systems. The focus of the course is an in-depth explanation of each NIST SP 800-53 Revision 3 controls and includes unclassified policies and procedures related to NSS to include what method should be used to test and validate each security control in accordance with NIST SP 800-53A and NIST SP 800-115, what evidence should be gathered, and how to more efficiently and effectively test Federal systems and infrastructure. The curriculum will introduce the independent tester or Validator to test the process for any of the NSS IA controls using manual and automated tests to ensure all controls are tested properly.

The CNSS/NIST Validator Course will cover NIST SP 800-53A, NIST SP 800-53 Revision 3, NIST SP 800-115, NIST SP 800-37, NIST SP 800-39 and the development of the Security Assessment Report (SAR), and Plan Of Action and Milestones (POA&M). The student will have a hands-on experience using scenario-based hands-on exercises in executing the validation tests with the approved tools. These exercises will include the development of the Security Assessment Report (SAR).

Lunarline's courseware has been evaluated and is the only industry training certified by the NSA/CNSS to meet NSTISSI No. 4011 and 4015 requirements. All of our instructors have hands-on, real world experience – you get more than just classroom instruction, you receive the benefits of actual expertise in executing these processes.

This course includes the following takeaway items: A printed training manual, a CD with a comprehensive set of NIST and Director of National Intelligence (DNI) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the Applying the CNSS/NIST Risk Management Framework / 800-53 Security Controls Validator 5 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

Page 9 of 15

GSA Schedule 70 Refresh 26 Training Course Descriptions (SIN 132-50)

Applying the CNSS/NIST Risk Management Framework In-Depth 3 Day

Certified Committee on National Security Systems

OVERVIEW:

This course equips the student with an overview of the system authorization process (also known as C&A) and the Risk Management Framework (RMF) for National Security Systems (NSS). In addition to the classroom instruction, the student will also participate in several scenario-based hands-on exercises in the implementation of the RMF to provide a clear knowledge bridge to the revised system authorization processes for those currently working with C&A for National Security Systems or for those who have limited or no C&A experience. These exercises will include the development of Systems Security Plans (SSPs), Security Assessment Reports (SARs), and Plans Of Action and Milestones (POA&Ms) for a NSS. This course meets the requirements of National Security Directive 42 (NSD-42), which outlines the roles and responsibilities for securing NSSs. The CNSS In-Depth Course will address the Federal and Intelligence Community requirements, including NIST SP 800-37, NIST SP 800-39, CNSS 1199 (DRAFT), and CNSS 1253 (DRAFT).

MODULES:

1. Critical Definitions and Policies
2. C&A Transformation/Transition Overview
3. The IC and the Transformation
4. Roles and Responsibilities
5. Accreditation Boundary
6. System Categorization

7. Select Security Controls
8. Implement, Document & Assess Security Controls
9. Authorize Information System
10. Monitor Information System
11. Reciprocity

Lunarline's CNSS/NIST classes include the following takeaway items: A printed training manual, a CD with a comprehensive set of NIST and Director of National Intelligence (DNI) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, "The Definitive Guide to the C&A Transformation" co-authored by Lunarline's VP of Cybersecurity and CEO.

Every student participating in the Applying the CNSS/NIST Risk Management Framework In- Depth 3 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow you to add the CNSS/NSA 4011 designation to your resumes.

Cybersecurity Fundamentals Workshop 4 Day

OVERVIEW:

This hands-on 3-day course provides participants with a high-level overview of various aspects of Cybersecurity in the context of a modern and Internet-connected environment. Through lecture, hands-on exercises, and group discussion, you will gain a foundational perspective on the challenges of designing a cybersecurity program, implementing secure systems, and other factors needed for a comprehensive cybersecurity solution. Upon completion of this course, each participant will be able to define cybersecurity terminology, compliance requirements, review sample attacks, and gain an understanding of the impact of current threat trends on cybersecurity implementation. This course is one of the core courses of Lunarline's Certificate Program in Cybersecurity.

Cybersecurity is one of the hottest issues for today's Federal and DOD Agencies and commercial organizations. Developed and developing nations, governments, defense departments and industries, and organizations in critical infrastructure verticals are being increasingly targeted by never-ending surges of cyber attacks from criminals and nation-states seeking information, economic or military advantage. The rapidity of the attacks is now so large and their level of sophistication so great, that many organizations are finding it difficult to identify which threats and vulnerabilities pose the greatest risk. They are faced with decisions on how resources should be allocated to ensure that the most likely and potentially damaging attacks are dealt with first. Exacerbating the problem is that most organizations do not have complete understanding of cybersecurity or an organizational approach to dealing with the challenges.

Every student participating in Lunarline's Cybersecurity Foundations course will receive a Certificate for successful participation in the course, which will allow you to claim 40 hours of Continuous Professional Experience for your existing certifications.

MODULES:

1. Introduction to Cybersecurity
2. Cybersecurity Laws, Regulations and Standards
3. Designing with Cybersecurity in Mind
4. Structures for Managing Cybersecurity
5. Special Cybersecurity Topics
6. Final Practical Exam/CAPSTONE Exercise

Lunarline's Cybersecurity Fundamentals class includes the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the

training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-authored by Lunarline’s VP of Cybersecurity and CEO.

Fundamentals of Software Assurance 3 Day

OVERVIEW:

This 3-day course provides participants with a high-level overview of various aspects of Software Assurance in the context of a modern and Internet-connected environment. Through lecture, hands-on exercises, and group discussion, you will gain a foundational perspective on the challenges of security software design and procurement, program, implementing secure software, and other factors needed for a comprehensive software assurance solution. Upon completion of this course, each participant will be able to define software assurance terminology, compliance requirements, review software assurance principles, and gain an understanding of the impact of current threat trends on security software implementation. This course is one of the core courses of Lunarline’s Certificate Program in Cybersecurity.

Secure assurance refers to the ability to ensure security personnel, software implementers, purchasers, and users that they can have a level of confidence that software will consistently operate in accordance with its intended goals. It includes software security, which is the process by which the software can operate effectively and security even when it comes under attack. Ideally, assured software will not contain faults or weaknesses that can be exploited either by human attackers or by the insertion (intentional or unintentional) of malicious or poor code.

MODULES:

1. Introduction to Software Assurance
2. Why is Software at Risk
3. Requirements for Secure Software
4. SwA Initiatives, Activities, and Organizations
5. Final Practical Exam/CAPSTONE Exercise

Every student participating in Lunarline’s Software Assurance course will receive a Certificate for successful participation in the course, which will allow you to claim 24 hours of Continuous Professional Experience for your existing certifications.

Lunarline’s Software Assurance(SwA) Best Practices class includes the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-authored by Lunarline’s VP of Cybersecurity and CEO.

Special Access Programs C&A Transition 3 Day

Special Access Programs/Sensitive Compartmented Information

OVERVIEW:

Lunarline’s SAP/SCI C&A Transition training provides students with a fundamental knowledge of the requirements for transitioning from the DIACAP/JAFAN/DCID C&A process to the NIST/CNSS requirements, as well as an in-depth look at the Risk Management Framework (RMF). This training equips the students with an in-depth indoctrination into the RMF and will provide them the requirements for managing risk, and ensuring that the confidentiality, availability and integrity of federal information and information systems is protected at a level commensurate with the security requirements of the information and the information system. Students will participate in a scenario-based hands-on exercise throughout the course to enhance understanding of the processes used for system authorization, including all of the elements of the Risk Management Framework.

The SAP/SCI C&A Transition Course crosswalks the current requirements of the DIACAP, JAFAN 6/3, and DCID 6/3 processes to the use of FIPS 199, NIST SP 800-60, NIST SP 800-37 Revision 1, NIST SP 800-39,

NIST SP 800-30, NIST SP 800-34, NIST SP 800-53 Revision 3, NIST SP 80053A, and CNSS 1253. All of our instructors have hands-on, real world experience – ensuring that you get more than just classroom instruction, but also receive the benefits of actual expertise in executing these processes.

Every student participating in Lunarline’s SAP/SCI C&A Transition course will receive a Certificate for successful participation in the course, which will allow you to claim 24 hours of Continuous Professional Experience credits for your existing certifications. Lunarline’s SAP/SCI C&A Transition class includes the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. You will also receive a copy of the book, “The Definitive Guide to the C&A Transformation” co-authored by Lunarline’s VP of Cybersecurity and CEO.

Page 13 of 15

FCIS-JB-980001-B Refresh: 26 Training Courses Descriptions

DoD 8570 Compliance CompTIA Security+ Certification 5 Day

OVERVIEW:

Lunarline, a CompTIA Authorized Partner, offers an intense 5 Day Security+ course consisting of nine lessons addressing each of the six Security+ domains in depth. All Lunarline training materials and books are CompTIA approved and have the most up to date information required to successfully understand the various security domains.

Students receive a CompTIA Security+ Deluxe Study Guide (which includes a CD), as well as CompTIA-approved course material that is composed of independent study assignments designed to help students prepare to successfully complete the Security+ exam.

The course was designed for students who are familiar with basic computer functionality, networking concepts and text-based interfaces and is taught exclusively by CTT+ and Security+ Certified Instructors with extensive real hands- on information security experience.

The primary objective of this 5 day course is to increase operator knowledge of physical, network and system security and prepare the student for the Security+ examination. Upon course completion, students should have an understanding of the Six security domains addressed by the Security+ certification. These domains include: Systems Security, Network Infrastructure, Access Control, Assessments and Audits, Cryptography, Organizational Security.

FEATURES: The Six Domains of Security+ - Systems Security - Network Infrastructure - Access Control - Assessments and Audits - Cryptography - Organizational Security

Every student participating in Lunarline’s Security+ 5-Day training will receive a test voucher for your Security+ Certification test. This course will prepare students to meet the certification compliance mandates required by DOD Directive 8570.1 for DOD information assurance technicians.

Recovery Planning Practitioner 5 Day

OVERVIEW:

This course is designed to provide an operational basis for all facets of recovery planning through information delivery and practical exercises. As a result of this course, students will be able to conduct risk analysis, business impact analysis, recovery strategy analysis and develop viable emergency response plans and recovery plans through the information obtained as a result of these assessments. Impart an ability to conduct Business Impact Analysis so that executive management will have a prioritized list of all functions performed, a determination of when the loss of a given function becomes unacceptable to the organization, and the resources necessary to enable the recovery of each function.

Provide students with insights into conducting Recovery Strategy Analysis, understanding the different strategies that are currently available and their applicability based on their strengths and weaknesses. This course will expose the students to emergency response techniques from the development of checklists to crafting concise communications releases. Upon completion of the study of recovery planning foundations,

this course will give the students a thorough knowledge of how to develop viable, easy-to-use recovery plans that address all hazards and all contingencies. Finally, this course is designed to provide the elements of an ongoing viable recovery capability through training and exercising programs that meet the needs of all audiences for all organizations.

MODULES:

1. Introduction
2. Risk Analysis
3. Business Impact Analysis
4. Recovery Strategy Analysis
5. Emergency Response Planning
6. Plan Development
7. Training Programs
8. Plan Exercise

This course includes the following takeaway items: A printed training manual, a CD with a comprehensive set of National Institute of Standards and Technology (NIST) - approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training.

CERTIFICATION:

This course prepares students for the National Institute for Business Continuity Management (NIBCM) Certified Continuity Manager (CCM) certification examination (additional cost, external testing entity).

No.	Lunarline Training	
	Price per Student	Price
001	DIACAP In-Depth Training	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$15,000.00
	Price for a group of 20-27 Students:	\$18,000.00
002	DIACAP Intensity Training	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$19,000.00
	Price for a group of 20-27 Students:	\$22,500.00
003	DIACAP IN-DEPTH WORKSHOP 5 DAY	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00
	Price for a group of 20-27 Students:	\$27,000.00
004	DIACAP VALIDATOR WORKSHOP 5 Day	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00
	Price for a group of 20-27 Students:	\$27,000.00
004	DIACAP Hands-On Overview 1 Day	
	Price per Student:	\$550.00
	Price for a group of 10-15 Students:	\$10,000.00
	Price for a group of 15-19 Students:	\$13,000.00
	Price for a group of 20-27 Students:	\$15,000.00
005	Applying the FISMA/NIST Risk Management Framework / 800-53 Security Controls Validator 5 Day	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00
	Price for a group of 20-27 Students:	\$27,000.00
006	Applying the FISMA/NIST Risk Management Framework In-Depth 3 Day	
	Price per Student:	\$1,500.00

	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$15,000.00
	Price for a group of 20-27 Students:	\$18,000.00
007	Applying the CNSS/NIST Risk Management Framework / 800-53 Security Controls Validator 5 Day	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00
	Price for a group of 20-27 Students:	\$27,000.00
008	Applying the CNSS/NIST Risk Management Framework In-Depth 3 Day	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$15,000.00
	Price for a group of 20-27 Students:	\$18,000.00
009	Cybersecurity Fundamentals Workshop 4 Day	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$19,000.00
	Price for a group of 20-27 Students:	\$22,500.00
010	Fundamentals of Software Assurance 3 Day	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$15,000.00
	Price for a group of 20-27 Students:	\$18,000.00
011	Special Access Programs C&A Transition 3 Day	
	Price per Student:	\$1,500.00
	Price for a group of 10-14 Students:	\$13,000.00
	Price for a group of 15-19 Students:	\$15,000.00
	Price for a group of 20-27 Students:	\$18,000.00
012	DoD 8570 Compliance CompTIA Security+ Certification 5 Day	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00
	Price for a group of 20-27 Students:	\$27,000.00
013	Recovery Planning Practitioner 5 Day	
	Price per Student:	\$2,400.00
	Price for a group of 10-15 Students:	\$18,000.00
	Price for a group of 15-19 Students:	\$23,000.00

	Price for a group of 20-27 Students:	\$27,000.00
--	--------------------------------------	-------------