

**GENERAL SERVICES ADMINISTRATION
FEDERAL SUPPLY SERVICE
AUTHORIZED FEDERAL SUPPLY SCHEDULE CATALOG/PRICE LIST**

On-line access to contract ordering information, terms and conditions, up-to-date pricing, and the option to create an electronic delivery order is available through GSA *Advantage!*, a menu-driven database system. The INTERNET address for GSA *Advantage!* is <http://www.gsaadvantage.gov>

SCHEDULE TITLE: IT Schedule 70 – GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT, SOFTWARE, AND SERVICES

CONTRACT NUMBER: GS-35F-0392X

CONTRACT PERIOD: May 18, 2011 – May 17, 2021

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

CONTRACTOR: Lunarline, Inc.
3300 Fairfax Drive, Suite 212
Arlington, VA 22201
Phone: (571) 481-9300
Fax: (202) 315-3003
Email: bizdev@lunarline.com

CONTRACTOR'S ADMINISTRATION SOURCE: Charlie Russell or Christine Marshall
VP of Finance, Accounting Manager
Lunarline, Inc.
3300 Fairfax Drive, Suite 212
Arlington, VA 22201
Phone: (571) 481-9300
Fax: (202) 315-3003
Email: accounting@lunarline.com

BUSINESS SIZE: Small Business

CUSTOMER INFORMATION:

1a. TABLE OF AWARDED SPECIAL ITEM NUMBERS (SINs):

SIN	Description
132-50	Training Courses
132-51	Information Technology Professional Services

1b. LOWEST PRICED MODEL NUMBER AND PRICE FOR EACH SIN: N/A

1c. HOURLY RATES: See pricelist below.

2. MAXIMUM ORDER*: \$500,000/Order

*If the best value selection places your order over the Maximum Order identified in this catalog/price list, you have an opportunity to obtain a better schedule contract price. Before placing your order, contact the aforementioned contractor for a better price. The contractor may (1) offer a new price for this requirement (2) offer the lowest price available under this contract or (3) decline the order. A delivery order that exceeds the maximum order may be placed under the schedule contract in accordance with FAR 8.404.

3. MINIMUM ORDER: \$100

4. GEOGRAPHIC COVERAGE: Domestic within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories.

5. POINT(S) OF PRODUCTION: N/A – Professional & Subscription Services Only

6. TERMS REGARDING MANUFACTURERS' END-USER LICENSE AGREEMENTS (FOR SOFTWARE ONLY): This contract, or the warranties guaranteed hereunder, is in no way affected, altered, or modified by any Manufacturer End-User License Agreement, unless the Contracting Officer has expressly incorporated a "Government" User End Licensing Agreement into the Contract. The terms of any "Commercial, Special or Other" user licensing agreement that has not been officially incorporated herein are applicable only to the Contractor-Manufacturer relationship, and do not alter the Government's rights or the Contractor's obligations under this contract.

7. BASIS OF AWARD CONTRACT TERMS: GSA Net Prices are shown on the attached GSA Pricelist. Negotiated discount has been applied and the IFF has been added.

Quantity/Volume Discount: SIN 132-50: None
SIN 132-51: 1% for Orders at or Exceeding \$100,000
3% for Orders at or Exceeding \$500,000

8. PROMPT PAYMENT TERMS: 1% 20 Days, Net 30

9a. Government Purchase Cards are accepted at or below the micro-purchase threshold.

9b. Government Purchase Cards are NOT accepted above the micro-purchase threshold.

10. FOREIGN ITEMS/TRADE AGREEMENTS ACT COMPLIANCE: None; the items herein are TAA Compliant. The information used by the Contracting Officer to make this determination was provided by the vendor and verified using all information available to the Government.

- 11a. TIME OF DELIVERY: 30 DARO
- 11b. EXPEDITED DELIVERY: N/A
- 11c. OVERNIGHT AND 2-DAY DELIVERY: N/A
- 11d. URGENT REQUIRMENTS: Agencies can contact the Contractor's representative to affect a faster delivery. Customers are encouraged to contact the contractor for the purpose of requesting accelerated delivery.

12. FOB POINT: Destination

Note: All travel required in the performance of this contract and orders placed hereunder must comply with the Federal Travel Regulations (FTR) or Joint Travel Regulations (JTR), 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. The contractor shall not add the Industrial Funding Fee onto travel costs. (FOB Terms noted above)

- 13a. ORDERING ADDRESS: Lunarline, Inc.
3300 Fairfax Drive, Suite 212
Arlington, VA 22201
- 13b. ORDERING PROCEDURES: For supplies and services, the ordering procedures, information on Blanket Purchase Agreements (BPA's) are found in Federal Acquisition Regulation (FAR) 8.405-3.
- 14. PAYMENT ADDRESS: Lunarline, Inc.
3300 Fairfax Drive, Suite 212
Arlington, VA 22201
- 15. WARRANTY PROVISION: N/A
- 16. EXPORT PACKING CHARGES: N/A
- 17. TERMS AND CONDITIONS OF GOVERNMENT PURCHASE CARD ACCEPTANCE: Accepted at or below the micro-purchase level.
- 18. TERMS AND CONDITIONS OF RENTAL, MAINTENANCE, AND REPAIR (IF APPLICABLE): N/A
- 19. TERMS AND CONDITIONS OF INSTALLATION (IF APPLICABLE): N/A
- 20a. TERMS AND CONDITIONS OF REPAIR PARTS INDICATING DATE OF PARTS PRICE LISTS AND ANY DISCOUNTS FROM LIST PRICES (IF AVAILABLE): N/A

- 20b. TERMS AND CONDITIONS FOR ANY OTHER SERVICES (IF APPLICABLE): N/A
- 21. LIST OF SERVICE AND DISTRIBUTION POINTS (IF APPLICABLE): N/A
- 22. LIST OF PARTICIPATING DEALERS (IF APPLICABLE): N/A
- 23. PREVENTIVE MAINTENANCE (IF APPLICABLE): N/A
- 24a. SPECIAL ATTRIBUTES SUCH AS ENVIRONMENTAL ATTRIBUTES (e.g. recycled content, energy efficiency, and/or reduced pollutants): N/A
- 24b. SECTION 508 COMPLIANCE FOR EIT: N/A
- 25. DUNS NUMBER: 14-7181569
- 26. NOTIFICATION REGARDING REGISTRATION IN SAM: Contractor is registered and valid in SAM.

GSA Price List

SIN 132-51		
S No.	Labor Category	Rate/Hour
1	Analyst (Business/System/Data)	\$ 129.24
2	Application Analyst	\$ 70.82
3	Application Developer - Senior	\$ 117.22
4	Application Developer - Mid	\$ 93.17
5	Application Developer - Junior	\$ 74.54
6	Application Integration Specialist	\$ 139.26
7	Certification Specialist - Senior	\$ 94.07
8	Certification Specialist - Mid	\$ 78.38
9	Certification Specialist - Junior	\$ 62.70
10	Computer System Security Specialist	\$ 86.49
11	Configuration Management Specialist	\$ 89.16
12	Database Administrator	\$ 133.24
13	Database Designer	\$ 129.24
14	Enterprise Architect - Senior	\$ 135.98
15	Enterprise Architect - Mid	\$ 113.32
16	Enterprise Architect - Junior	\$ 97.27
17	Help Desk Analyst	\$ 49.11
18	Information Assurance Engineer - Senior	\$ 129.24
19	Information Assurance Engineer - Mid	\$ 80.27
20	Information Assurance Engineer - Junior	\$ 73.66
21	Information Security Analyst - Senior	\$ 133.24
22	Information Security Analyst - Mid	\$ 92.59
23	Information Security Analyst - Junior	\$ 51.94
24	Information Security Engineer - Senior	\$ 149.27
25	Information Security Engineer - Mid	\$ 68.94
26	Information Security Engineer - Junior	\$ 55.15
27	Information System Security Specialist	\$ 153.52
28	Internet Developer - Senior	\$ 123.23
29	Internet Developer - Mid	\$ 97.18
30	IT Subject Matter Expert	\$ 143.26
31	IT Technologist	\$ 99.15
32	Network Engineer - Senior	\$ 133.24
33	Network Engineer - Mid	\$ 97.18
34	Network Security Specialist	\$ 139.26
35	Penetration Tester - Senior	\$ 90.66
36	Penetration Tester - Junior	\$ 75.55
37	Program Manager	\$ 139.26
38	Project Control Analyst	\$ 137.75
39	Project Manager	\$ 139.26
40	Quality Assurance Specialist	\$ 129.24
41	R&D Specialist	\$ 147.76

42	Security Subject Matter Expert	\$ 147.76
43	Software Tester	\$ 93.17
44	System Administrator	\$ 133.24
45	System/Software Architect	\$ 134.25
46	Technical Instruction Specialist	\$ 89.16
47	Technical Writer - Mid	\$ 68.56
48	Technical Writer - Junior	\$ 57.13
49	Web Specialist	\$ 139.26

SIN 132-50		
S No.	Course Title	Rate/Class
DIACAP Hands-On Overview 1 Day:		
50	1 Student	\$ 555.79
DIACAP Hands-On In-Depth 3 Day:		
51	1 Student	\$ 1,515.78
52	6 to 9 Students	\$10,154.74
53	10 to 15 Students	\$13,186.31
54	16 to 19 Students	\$15,207.35
55	20 to 29 Students	\$18,238.92
DIACAP Hands-On Intensity 4 Day:		
56	1 Student	\$ 2,021.05
57	6 to 9 Students	\$12,681.05
58	10 to 15 Students	\$15,712.61
59	16 to 19 Students	\$19,249.44
60	20 to 29 Students	\$27,333.62
DIACAP In-Depth Workshop 5 Day:		
61	1 Student	\$ 2,425.25
62	6 to 9 Students	\$15,257.88
63	10 to 15 Students	\$18,289.45
64	16 to 19 Students	\$23,342.06
65	20 to 29 Students	\$27,384.15
DIACAP Validator Workshop 5 Day:		
66	1 Student	\$ 2,425.25
67	6 to 9 Students	\$15,257.88
68	10 to 15 Students	\$18,289.45
69	16 to 19 Students	\$23,342.06
70	20 to 29 Students	\$27,384.15
8570 Compliance CompTIA Security+ Certification 5 Day:		
71	1 Student	\$ 2,501.04
72	6 to 9 Students	\$23,342.06
73	10 to 15 Students	\$25,363.10
74	16 to 19 Students	\$28,394.67
75	20 to 29 Students	\$31,426.24
Cybersecurity Fundamentals Workshop 4 Day:		
76	1 Student	\$ 2,021.05

Fundamentals of Software Assurance:		
77	1 Student	\$ 1,515.78
Recovery Planning Practitioner COOP 5 Day:		
78	1 Student	\$ 2,425.25
Cyber Tools and Analysis Workshop 4 Day:		
79	1 Student	\$ 2,021.05
Applying the FISMA/NIST RMF In-Depth 3 Day:		
80	1 Student	\$ 1,515.78
81	6 to 9 Students	\$10,154.74
82	10 to 15 Students	\$13,186.31
83	16 to 19 Students	\$15,207.35
84	20 to 29 Students	\$18,238.92
Applying the FISMA/NIST RMF Intensity 4 Day:		
85	1 Student	\$ 2,021.05
Applying the FISMA/NIST RMF / 800-53 Security Controls Validator 5 Day:		
86	1 Student	\$ 2,425.25
87	6 to 9 Students	\$15,257.88
88	10 to 15 Students	\$18,289.45
89	16 to 19 Students	\$23,342.06
90	20 to 29 Students	\$27,384.15
Applying the CNSS/NIST RMF In-Depth 3 Day:		
91	1 Student	\$ 1,515.78
92	6 to 9 Students	\$10,154.74
93	10 to 15 Students	\$13,186.31
94	16 to 19 Students	\$15,207.35
95	20 to 29 Students	\$18,238.92
Applying the CNSS/NIST RMF Intensity 4 Day:		
96	1 Student	\$ 2,021.05
Applying the CNSS/NIST RMF / 800-53 Security Controls Validator 5 Day:		
97	1 Student	\$ 2,425.25
98	6 to 9 Students	\$15,257.88
99	10 to 15 Students	\$18,289.45
100	16 to 19 Students	\$23,342.06
101	20 to 29 Students	\$27,384.15

Labor Category Descriptions

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

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: Perform information technology analysis activities to support business decisions relative to the development, enhancement, and maintenance of products and services applicable to multiple lines of business. Responsible for technically analyzing business processes, data and/or information systems, including analysis of system architecture and associated hardware/software, e.g., functional implementation of each application, database(s), platform(s), etc. Data analysis, including reliability, integrity, etc., associated processes, business logic, etc., is also included. Anticipate and identify user problems and needs. Recommend business solutions based on analysis activities, customer requirements, industry trends, and best practices/authoritative guidance. Lead, plan, schedule, and control complex projects and activities with customers, support groups, and vendors on concurrent projects. Apply extensive business and industry knowledge to develop project specifications. Advise on methods to improve business processes and remove non-value added activities. Coordinate and participate in proposals, feasibility studies, implementations, and new business development. Lead training activities for knowledge transfer, and build relationships with multiple customer/business levels.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor's degree in disciplines other than those listed above may be considered if and only if they have at least eight (8) years of experience in analyzing the business processes and information systems of organizations.

2. Commercial Job Title: Application Analyst

Technical Qualifications/Experience: Overall three (3) years of experience in analyzing the software applications for their functionality, monitoring performance, identifying bottlenecks and recommending measures to improve application performance.

Functional Responsibility: Work with Software Design and Development groups to analyze software applications for functionality, performance and integration with other systems. Monitor application performance, identify bottlenecks and recommend measures to improve application performance.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Business, Mathematics or Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of experience in analyzing the software applications of organizations.

3. **Commercial Job Title: Application Developer - Senior**

Technical Qualifications/Experience: Minimum six (6) years of experience in supervising and mentoring other Application Developers in the performance of detailed analysis, building software development tools and producing highly technical programs such as cross-compilers and communications software operating systems. Must be proficient in programming in the relevant programming language/s, e.g., Java, XML, .Net, Web Methods, C, C++, Perl, COBOL, Oracle PL/SQL, Unix Shell scripting.

Functional Responsibility: Lead business logic and data modeling activities associated with application development. Direct the activities of programmers and analysts in the performance of detailed analysis, 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. Supervise and participate in the development of manuals and user guides for programmers and operating staff. Establish and supervise software design efforts necessary to integrate new hardware and code programs in applicable languages using standard requirements documentation, e.g., detailed flow diagrams, input/output descriptions, performance specifications, etc. Supervise software analysis, the development of program specifications and the development of program code. Perform implementation tasks and direct the conduct of application testing to insure results. Direct and participate 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in supervising and mentoring Application Developers in the performance of detailed analysis, building software development tools, and producing highly technical programs such as cross-compilers and communications software operating systems.

4. **Commercial Job Title: Application Developer - Mid**

Technical Qualifications/Experience: Minimum four (4) 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: Assist in the logic behind and the data modeling associated with application development. Perform 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. Work independently in support of joint applications development efforts. 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, mobile devices, and other emerging technology platforms.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry applications.

5. Commercial Job Title: Application Developer - Junior

Technical Qualifications/Experience: Minimum two (2) 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: Assist in the logic behind and the data modeling associated with application development. Perform 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. Work independently in support of joint applications development efforts. 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, mobile devices, and other emerging technology platforms.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry applications.

6. Commercial Job Title: Application Integration Specialist

Technical Qualifications/Experience: Minimum six (6) 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. Has the proven ability to work well independently with minimal supervision.

Functional Responsibility: Provide computer systems expertise relative to automated information system(s) integration with existing infrastructure, architecture, and/or other systems. Perform systems analysis, alternative solutions, and design of technical and business solutions. Under minimal guidance and supervision, conduct project feasibility and implementation studies, including the development project plans, testing methodologies/plans, and overarching project management documentation. Develop and implement data conversion routines. Perform/direct system testing to insure satisfactory results within requirements. Duties require knowledge of data sources, data flow, system interactions, computer equipment, including hardware and software applications. Provide technical support to the project team. Establish and maintain development, testing environments and configuration management processes and structures. Serve as primary point-of-contact for third party software and hardware vendors.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, Economics, or Mathematics. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least eight (8) 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.

7. Commercial Job Title: Certification Specialist - Senior

Technical Qualifications/Experience: Overall three (3) years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc..

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. Candidates having a bachelor's degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.

8. Commercial Job Title: Certification Specialist - Mid

Technical Qualifications/Experience: Overall three (3) years of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses,

systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc..

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. Candidates having a bachelor's degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.

9. Commercial Job Title: Certification Specialist - Junior

Technical Qualifications/Experience: Overall one (1) year of experience in assessing, analyzing, evaluating, validating, certifying and accrediting, etc., various businesses, systems, software development processes, etc., relative to one or more compliance standard, security controls/requirements, etc.

Functional Responsibility: Responsible for evaluating various businesses, systems, software development processes, etc., validating against standard requirements and/or compliance controls, e.g., ISO, CMMI, HIPAA/HITECH, NIST, DIACAP, DODIIS/DCID, CNSS, ICD 503, etc. Responsible for assisting in the scoping effort relative to the target compliance activity. Assist in the development of the compliance methodology based on experience as well as best practices associated with target compliance activity. Document tasks to justify compliance, bring target into compliance (both technically and non), and present compliance package for approval by clients and/or approval chains as is appropriate. Analyze and evaluate the security requirements/controls in an organization, validating them with standard security guidelines and policies, and certifying that all information systems are compliant with standard security guidelines.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related degree. Candidates having a bachelor's degree in disciplines other than those listed above may be considered if and only if they have at least four (4) years of relevant experience.

10. Commercial Job Title: Computer System Security Specialist

Technical Qualifications/Experience: Minimum three (3) years of experience in defining, implementing and maintaining the information security for businesses, business units,

divisions, organizations, agencies, etc. Must have strong knowledge of encryption, intrusion detection/prevention, network security, and ethical hacking/penetration testing.

Functional Responsibility: Responsible for ensuring that the organization's networks, as well as information, is secure. Employ continuous monitoring of intrusion detection/prevention and other perimeter defense devices. Ensure appropriate data encryption (in transit and at rest) levels based on protection needs of targeted data. Maintain awareness of system/network security posture to include vulnerability scanning to facilitate application of quick and effective corrective measures, while ensuring configuration management requirements are met. Provide technical knowledge and information assurance analysis support, to include security assessment of applications; operating systems; internet-facing interfaces, intranet and other interconnections. Strong knowledge of best practices associated with as well as appropriate authoritative guidance for physical security; network security; security risk assessments; critical infrastructure protection; continuity and contingency planning; emergency preparedness; security awareness and training. Provide analysis of existing systems vulnerabilities including possible intrusion/entry points, resource manipulation, denial of service, and/or destruction of resources. Provide technical support and analysis to document organizational information protection framework, and support policy and procedures preparation and implementation.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering, or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least five (5) years of experience in analyzing, designing, implementing, integrating and maintaining computer/information systems security postures.

11. Commercial Job Title: Configuration Management Specialist

Technical Qualifications/Experience: Minimum four (4) 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, Visual SourceSafe, or other CM tool.

Functional Responsibility: Support the development and maintenance of configuration management plans, processes, procedures, etc., 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. Requires minimal supervision; however overarching strategic direction must be provided. 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.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be

considered if and only if they have at least five (5) years of experience in performing configuration management and version control tasks.

12. Commercial Job Title: Database Administrator

Technical Qualifications/Experience: Five (5) years of general experience including two (2) years specialized experience. Serves in a supervisory manner, has responsibility for junior staff tasking/development, also serves as a management interface. Two of the five 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 or similar.

Functional Responsibility: Responsible for building/installing databases on servers/clients. Maintain and create users, nodes, instances, databases, tablespaces, containers, bufferpools and logs. Migrate data between databases. Extract data from one system into flat files and then load into the database without constraints. Write stored procedures, and triggers to populate data from non-constraints tables to normalized tables with constraints. Tune 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. Analyze the execution path of the query to determine the cost, indexing and cardinality. Write scripts to create instances, databases, scheduling online, offline backups and restoring databases. Implement Active Standby Clustering, database partitioning using utilities. Provide highly technical expertise and guidance in the design, implementation, operation and maintenance of database management systems (DBMS). Evaluate and recommend available DBMS products after matching requirements with system capabilities. Determine file organization, indexing methods, and security procedures for specific applications. Control the design and use of databases. Control the global view of databases, control the access to the databases, assure the safekeeping of the databases (from accidental or intentional damage or loss), and monitor 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. Evaluate and recommend available DBMS products after matching requirements with system capabilities. Prepare and deliver presentations on DBMS concepts.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in database administration.

13. Commercial Job Title: Database Designer

Technical Qualifications/Experience: Minimum five (5) years of 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). Analyze the database systems and programs,

which include access methods, access time, file structures, device allocation, validation checks, statistical methods, and security. Will also work with the 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, Engineering (Electrical, Computer, Mechanical) or related degree. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience analyzing and designing databases.

14. Commercial Job Title: Enterprise Architect - Senior

Technical Qualifications/Experience: Minimum six (6) years of experience in enterprise system architecture.

Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with business and technology direction and objectives. Develop information technology technical and application architectures and participate in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually review 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, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

15. Commercial Job Title: Enterprise Architect - Mid

Technical Qualifications/Experience: Minimum four (4) years of experience in enterprise system architecture.

Functional Responsibility: Contribute to the establishment and maintenance of an overall IT architecture relevant to and consistent with business and technology direction and objectives. Develop IT technical and application architectures and participate in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop recommendations and requirements for legacy applications to evolve towards conformance with target architecture. Continually review 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, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

16. Commercial Job Title: Enterprise Architect - Junior

Technical Qualifications/Experience: Minimum two (2) years of experience in enterprise system architecture.

Functional Responsibility: Support the Enterprise Architect in designing and maintaining overall enterprise system architecture relevant to and consistent with business and technology direction and objectives. Under the guidance of the Enterprise Architect, facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Must have a basic understanding of networking architectures.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of relevant experience.

17. Commercial Job Title: Help Desk Analyst

Technical Qualifications/Experience: Minimum two (2) years of experience in providing help desk support on various problems and issues related to application software, information systems and processes support functions such as assisting users and system developers with issues and problems in system operation.

Functional Responsibility: Responsible for providing first and second level help desk support to solve problems related to the operations and performance of software applications, operating systems, databases, networks and functional understanding. Provide software support functions like code maintenance, backups, functionality modifications, reports generation, modify/upgrade software documentation, user training, software migrations, version control, technical support and user training.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering or a related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

18. Commercial Job Title: Information Assurance Engineer - Senior

Technical Qualifications/Experience: Minimum six (6) years of experience in defining IS Security policies, analyzing, designing, implementing, integrating and maintaining the information security of firms.

Functional Responsibility: Analyze and define security requirement for computer systems which may include mainframes, workstations, and personal computers. Design, develop, engineer, and implement solutions that meet security requirements. Provide integration and implementation of the computer system security solution. Establish and satisfy complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Support customers at the highest levels in the development and implementation of doctrine and policies. Apply 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above will also be considered if and only if they have at least six (6) years of experience in analyzing, designing, implementing, integrating and maintaining the Information Security of firms.

19. Commercial Job Title: Information Assurance Engineer - Mid

Technical Qualifications/Experience: Minimum three (3) years of experience in documenting and analyzing IS security policies, implementing, integrating and maintaining the information security of firms.

Functional Responsibility: Analyze and define security requirement for computer systems which may include mainframes, workstations, and personal computers. Design, develop, engineer, and implement solutions that meet security requirements. Provide integration and implementation of the computer system security solution. Establish and satisfy complex system-wide information security requirements based upon the analysis of user, policy, regulatory, and resource demands. Support customers at the highest levels in the development and implementation of doctrine and policies. Apply 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least five (5) years of experience in analyzing, designing, implementing, integrating and maintaining the information security of firms.

20. Commercial Job Title: Information Assurance Engineer - Junior

Technical Qualifications/Experience: Minimum two (2) years of experience in documenting and analyzing IS security policies, implementing, integrating and maintaining the information security of firms.

Functional Responsibility: Support the Information Assurance Engineer in implementing, and maintaining the information systems security policies and procedures previously defined by the Information Assurance Engineer along with the Technical Management of large

organizations. Implement solutions that meet security requirements. Provide integration and implementation of the computer system security solution. Apply 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of experience in analyzing, designing, implementing, integrating and maintaining the Information Security of firms.

21. Commercial Job Title: Information Security Analyst – Senior

Technical Qualifications/Experience: Minimum eight (8) years of experience in analyzing computer security at large firms, conducting gap analysis, identifying and alleviating potential loopholes.

Functional Responsibility: Analyze the client system security, conduct gap analysis, determine enterprise information security standards, and develop and implement information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least seven (7) years of experience in analyzing computer security at large firms.

22. Commercial Job Title: Information Security Analyst - Mid

Technical Qualifications/Experience: Minimum five (5) years of experience in analyzing computer security at large firms, conducting gap analysis, identifying and alleviating potential loopholes.

Functional Responsibility: Analyze the client system security, conduct gap analysis, determines enterprise information security standards, and develop and implement information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above will also be considered if and only if they have at least seven (7) years of experience in analyzing computer security at large firms.

23. Commercial Job Title: Information Security Analyst - Junior

Technical Qualifications/Experience: Minimum one (1) year of experience in analyzing computer security at large firms, conducting gap analysis, identifying and alleviating potential loopholes.

Functional Responsibility: Support the Information Security Analysts. Analyze the client system security, conduct gap analysis, determine enterprise information security standards, and develop and implement information security standards and procedures.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least four (4) years of experience in analyzing computer security at large firms.

24. Commercial Job Title: Information Security Engineer – Senior

Technical Qualifications/Experience: Minimum eight (8) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

Functional Responsibility: Responsible for defining/ameliorating the IS Policy, including the 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. Provide 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. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conducts gap analysis, determines enterprise information security standards, and develops and implements information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in defining, implementing and maintaining the information security of firms.

25. Commercial Job Title: Information Security Engineer – Mid

Technical Qualifications/Experience: Minimum five (5) years of experience in defining, implementing and maintaining the information security of firms. Must have a strong know-how of encryption, intrusion detection, network security and ethical hacking.

Functional Responsibility: Responsible for defining/ameliorating the IS Policy, including the 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. Provide 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. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Analyze the client system security, conduct gap analysis, determine enterprise information security standards, and develop and implement information security standards and procedures. Ensure that all information systems are functional and secure.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least eight (8) years of experience in defining, implementing and maintaining the information security of firms.

26. Commercial Job Title: Information Security Engineer - Junior

Technical Qualifications/Experience: Minimum two (2) years of experience in defining, implementing and maintaining the information security of firms. Must have a 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. Provide 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. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitors firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be

considered if and only if they have at least ten (10) years of experience in defining, implementing and maintaining the information security of firms.

27. Commercial Job Title: Information System Security Specialist

Technical Qualifications/Experience: Minimum ten (10) 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 the IS Policy of an organization. Also responsible for ensuring that the organization networks as well as information is secure at all times, constantly monitoring the intrusion detection, data encryption, and for taking quick and effective corrective measures in the event of a breach. Provide 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. Provide analysis of existing system's vulnerability to possible intrusions, resource manipulation, resource denial and destruction of resources. Provide technical support and analysis to document organizational information protection framework, and supports policy and procedures preparation and implementation. Monitor firewall logs. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, creates monitoring reports and logs and ensure functionality of links. Establish backups and monitor site security.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics or Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least fourteen (14) years of relevant experience.

28. Commercial Job Title: Internet Developer - Senior

Technical Qualifications/Experience: Minimum 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. Analyze, design, develop and test internet applications using languages like Microsoft .Net, Java, XML, JSP, EJB and Javascript and deploy 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).

29. Commercial Job Title: Internet Developer - Mid

Technical Qualifications/Experience: Minimum 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, and CORBA.

Functional Responsibility: Analyze, understand the architecture and develop 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of experience in independently developing industry internet/web applications.

30. Commercial Job Title: IT Subject Matter Expert

Technical Qualifications/Experience: Minimum five (5) 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 developing the system architecture.

Functional Responsibility: Responsible for serving as facilitator for Integrated Product Team, defining/ameliorating the policies and procedures of an organization, process or program. Utilize 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 developing the system architecture. 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, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least nine (9) 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.

31. Commercial Job Title: IT Technologist

Technical Qualifications/Experience: Minimum four (4) years of technical experience in IT systems, and Application Integration.

Functional Responsibility: Responsible for ensuring a stable and usable system through the integration of various software and hardware platforms and components. Provide technical support to the project team. Establish and maintain development and testing environments and the configuration management process and structures. Serve as point-of-contact for third-party software and hardware vendors. Responsible for providing software support functions like code maintenance, backups, functionality modifications, reports generation, modify/upgrade software documentation, user training, software migrations, version control, technical support and user training.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

32. Commercial Job Title: Network Engineer - Senior

Technical Qualifications/Experience: Minimum 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 interconnectivity 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. Provide system administration of Network, Web, and/or communications systems, including Local Area Network (LAN), Wide Area Network (WAN). Maintain servers, create monitoring reports and logs and ensure functionality of links. Establish backups and monitor site security. Responsible for developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms. Design, develop, test and implement new system software modules and enhancements to current systems; design, develop, test, and implement diagnostic utilities to analyze and report system status and performance. Evaluate 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, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least eight (8) years of experience in planning, management, support, and operation of the LAN/WAN environment.

33. Commercial Job Title: Network Engineer - Mid

Technical Qualifications/Experience: Minimum 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 the 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. Design, develop, test and implement new system software modules and enhancements to current systems; design, develop, test, and implement diagnostic utilities to analyze and report system status and performance. Monitor and evaluate overall system performance of operating system facilities, software products, computer services, and communications and networking facilities. Specify, install 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, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in developing, refining, and troubleshooting a large distributed environment, involving UNIX and MS-DOS platforms.

34. Commercial Job Title: Network Security Specialist

Technical Qualifications/Experience: Minimum five (5) years of experience in installing, configuring, and maintaining organization's operating systems, and network components to ensure security of networks.

Functional Responsibility: Install, configure and maintain organization's operating systems. Analyze and resolve problems associated with server hardware, NT, applications software. Detect, diagnose, and report NT related problems on both NT server and NT desktop systems. Perform a wide variety of tasks in software/hardware maintenance and operational

support of NT Server systems. Analyze general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Design, develop, engineer, and implement solutions that meet network security requirements. Perform 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) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least seven (7) years of relevant experience in installing, configuring, and maintaining organization's operating systems, and network components.

35. Commercial Job Title: Penetration Tester - Senior

Technical Qualifications/Experience: Minimum five (5) years of experience in independently performing penetration testing using automated tools to determine potential security breaches, and detect any intrusion into the organization's Information Systems by hackers or viruses.

Functional Responsibility: Responsible for performing penetration testing on organizational systems, data and networks using automated tools like TripWire to determine potential internet or information security breaches, and detect any intrusion into the organization's information systems by hackers or viruses. Responsible for following the penetration test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify breaches, or potential breaches and the root causes of such breaches.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, Mathematics or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in performing penetration testing, and intrusion detection using automated tools like Tripwire.

36. Commercial Job Title: Penetration Tester - Junior

Technical Qualifications/Experience: Minimum two (2) years of experience in independently performing penetration testing using automated tools to determine potential security breaches, and detect any intrusion into the organization's Information Systems by hackers or viruses.

Functional Responsibility: Responsible for performing penetration testing on organizational systems, data and networks using automated tools like TripWire to determine potential internet or information security breaches, and detect any intrusion into the organization's information systems by hackers or viruses. Responsible for following the penetration test plan, conducting the unit as well as system testing as per pre-defined test cases, complete test reporting documentation, identify breaches, or potential breaches and the root causes of such breaches.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, Mathematics or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) years of experience in performing penetration testing, and intrusion detection using automated tools like Tripwire.

37. Commercial Job Title: Program Manager

Technical Qualifications/Experience: Minimum eight (8) years of experience in the IT industry, out of which at least 5 years must be in the field of Project Management, Business Administration, Human Resources, and/or Client Relationship Management.

Functional Responsibility: Act as the central point of contact with the Contracting Officer, Contracting Officer's Representative and Task Managers. Responsible for coordinating the management of all work performed on this contract, including subcontractors, team members, and vendors. Keep 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 facilitate 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 to 3 years of additional experience. Master's Degree in Computer Science; Master's Degree in Business Administration is desirable.

38. Commercial Job Title: Project Control Analyst

Technical Qualifications/Experience: Minimum four (4) years of experience in analyzing the project schedules and costs. Must have a thorough knowhow of Software Development Lifecycle, and proficiency in Project Management tools like MS Project, tools like Visio, MS Word, Excel and Power Point.

Functional Responsibility: Assist the Project Manager in analyzing the project schedules, and costs. Monitor and analyze each project task and sub task using automated tools like MS Project, identifies potential sources of project delays and cost over-runs and reports the results to the Project Manager. Also analyze the utilization and productivity of each project resources, and identify potential bottlenecks.

Minimum Education: Bachelor's degree in Accounting, Business Administration or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience in analyzing the project schedules and costs.

39. Commercial Job Title: Project Manager

Technical Qualifications/Experience: Minimum five (5) years of experience in managing IT 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: Responsible for the timely execution of the various Task Order projects awarded under the master contract. 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. Maintain project status documentation, give regular updates to the account manager, give technical presentations to the client representatives and periodically attends status meetings with the client representatives. Report to the Program Manager for the contract.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. A Master's degree in Computer Science is desirable. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least seven (7) years of experience in managing IT projects.

40. Commercial Job Title: Quality Assurance Specialist

Technical Qualifications/Experience: Minimum 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: Provide 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. Provide 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. Perform regular internal audits to ensure proper quality control. 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, Public Administration or related field.

41. Commercial Job Title: R&D Specialist

Technical Qualifications/Experience: Minimum five (5) years of experience in researching data, technology, and available tools and develop IT solutions, tools and applications to better manage and run the IT projects and organization.

Functional Responsibility: Research data, software tools, technologies, methodologies, and IT solutions to potential problems faced by project and organizational teams. Develop, test and implement automated applications, tools, and systems in order to improve the efficiency of the organizational processes and/or better management and operations of IT projects.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above will also be considered if and only if they have at least seven (7) years of relevant experience.

42. Commercial Job Title: Security Subject Matter Expert

Technical Qualifications/Experience: Minimum five (5) years of experience in providing advice and guidance on various matters related to organizational security systems, IS Policy, potential vulnerabilities and solutions to fix these vulnerabilities.

Functional Responsibility: Utilize the knowhow, expertise and experience in the field of Information, Internet, System, and Network Security to assist the IS Specialist in defining proven Information Security Policy, and standards for various organizations. Also assist Information Security Analysts, Information Security Engineers, and Information Assurance Engineers in implementing the Information Security controls, detecting intrusion, conducting vulnerability assessments and finding solutions to fix potential weak spots for breaches.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering or related field. A degree in disciplines other than those listed above may also be considered if and only if they have at least six (6) years of relevant experience.

43. Commercial Job Title: Software Tester

Technical Qualifications/Experience: Minimum 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 Public Administration, or related field. Candidates having a bachelor's degree in disciplines other than those listed above will also be considered if they have at least seven (7) years of experience in performing unit and integration testing manually as well as using automated tools like Load Runner, WinRunner and Test Director.

44. Commercial Job Title: System Administrator

Technical Qualifications/Experience: Minimum five (5) 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.

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. Implement and support local area network (LAN) and campus area network (CAN) hardware and software. Analyze customer workflow and procedures to recommend operational support tools and technologies to satisfy customer needs. Act as a liaison between the customer, suppliers, and other technical groups to resolve network and hardware problems. Analyze performance problems and recommends solutions to enhance functionality, reliability and/or usability. Implement operational support standards and procedures relating to change management, performance management, and security. Recommend changes and improvements to existing standards. Develop site administration manual (SAM) documentation. Provide user orientation on hardware, software and network operations.

Minimum Education: Bachelor's degree in Computer Sciences, Information Systems, Mathematics, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if they have at least seven (7) 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.

45. Commercial Job Title: System/Software Architect

Technical Qualifications/Experience: Minimum eight (8) years of experience in the field of IT out of which at least 5 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. Design and develop new software products or major enhancements to existing software. Address problems of systems integration, compatibility, and multiple

platforms. Develop information technology technical and application architectures and participates in setting technology direction and standards. Provide technical architectural design review for major business applications and technology initiatives. Facilitate linkage with key business areas by understanding enterprise requirements and by communicating architecture frameworks best practices and standards. Develop 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, Engineering (Electrical, Computer, Mechanical) or related field. Candidates having a bachelor's degree in disciplines other than those listed above may also be considered if and only if they have at least ten (10) years of experience in architecting IT systems.

46. Commercial Job Title: Technical Instruction Specialist

Technical Qualifications/Experience: Minimum three (3) to seven (7) years of managing technology and security training programs including training documentation. Experience with multimedia aided instruction is preferred.

Functional Responsibility: Provide computer training and classroom instructions to users and staff personnel as appropriate. Gather 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. Evaluate effectiveness of instruction by ensuring students have a thorough knowledge of subject matter and hands-on skill at performing required task.

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

47. Commercial Job Title: Technical Writer - Mid

Technical Qualifications/Experience: Overall four (4) years of experience in preparing technical documents and manuals.

Functional Responsibility: Prepare technical documentation, including but not limited to, Technical System Manuals, Operation Manuals, Training documents, functional specifications, test and validation reports, and software application documents.

Minimum Education: Associate degree in any technical discipline.

48. Commercial Job Title: Technical Writer - Junior

Technical Qualifications/Experience: Minimum two (2) years of experience in preparing technical documents and manuals.

Functional Responsibility: Prepare technical documentation, including but not limited to, Technical System Manuals, Operation Manuals, Training documents, functional specifications, test and validation reports, and software application documents.

Minimum Education: Associate degree in any technical discipline.

49. Commercial Job Title: Web Specialist

Technical Qualifications/Experience: Minimum 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, Engineering (Electrical, Computer, Mechanical) or related field.

Training Course Descriptions

50. 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. This course provides an overview of DIACAP requirements, documentation, and associated processes.

Lunarline's DIACAP Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST - DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

51-55. 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:

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

Lunarline's DIACAP Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST - DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

56-60. 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:

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

Lunarline's DIACAP Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST - DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

61-65. 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)/Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow the student to add the NSA/CNSS 4011 designation to your resumes. This course is one of Lunarline's 3 qualifying classes to reach the NSA/CNSS NSTISSI 4015 designation.

Lunarline's DIACAP Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST - DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

66-70. 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:

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

Lunarline's DIACAP Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST - DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

71-75. 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.

Domains:

- Domain 1: Systems Security
- Domain 2: Network Infrastructure
- Domain 3: Access Control
- Domain 4: Assessments & Audits
- Domain 5: Cryptography
- Domain 6: Organizational Security

Lunarline's Security+ Classes Include the Following Takeaway Items: A test voucher for their 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 and managers.

76. Cybersecurity Fundamentals Workshop 4 Day

Overview: This hands-on 4 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, students 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.

Modules:

- Module 1: Introduction to Cybersecurity
- Module 2: Cybersecurity Laws, Regulations & Standards
- Module 3: Designing with Cybersecurity in Mind
- Module 4: Structures for Managing Cybersecurity
- Module 5: Special Cybersecurity Topics
- Module 6: Final Practical Exam/Capstone Exercise

Lunarline's Cybersecurity Fundamentals Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's Cybersecurity Foundations course will also receive a certificate for successful participation in the course, which will allow students to claim 40 hours of Continuous Professional Experience for their existing certifications.

77. Fundamentals of Software Assurance

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.

Modules:

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

Lunarline's Software Assurance Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's Software Assurance course will also receive a certificate for successful participation in the course, which will allow students to claim 24 hours of Continuous Professional Experience for their existing certifications.

78. Recovery Planning Practitioner COOP 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 analyses, business impact analyses, recovery strategy analyses and develop viable emergency response plans and recovery plans through the information obtained as a result of these assessments. The Recovery Planning Practitioner Course imparts an ability to conduct Business Impact Analyses 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.

The Recovery Planning Practitioner course provides 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 fundamentals, this course will give 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:

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

Lunarline's Recovery Planning Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-DoD approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training.

In addition, students will have the option to sit in on the Certified Continuity Manager (CCM) certification exam. Lunarline has partnered with the National Institute for Business Continuity Management (NIBCM), allowing students who have completed the Recovery Planning course to take this exam. When registering for the course and exam, students can choose either the public sector (COOP) or the private sector (Business Continuity Planning) specialty.

79. Cyber Tools and Analysis Workshop 4 Day

Overview: Do you want to better understand how to use cyber tools in securing networks? Would you like to be better prepared to answer fairly technical security questions about Microsoft Active Directory, Unix, Linux, databases, firewall, intrusion detection systems and major network services like the Domain Name Service? Would you like a combination of professional instruction and well-structured hands-on experiences securing these operating systems, applications and infrastructure?

This course concentrates on cyber security tools, operating systems, applications, network architectures and best practices in government and industry network security. The course

uses a fifty percent hands-on approach (25 lab experiences) to focus not only on tool deployment and operation system configuration, but cyber security network defense and analysis techniques. Students will configure multiple operating systems, practice network defense techniques, and understand attack prevention methods in a state of the art security lab. No experience is required; however an understanding of technical security controls or some previous experience with system administration will enhance learning.

Lunarline's Cyber Tools and Analysis Classes Include the Following Takeaway Items: A certificate for successful participation in this course, which will allow students to claim 32 hours of Continuous Professional Experience for their existing certifications.

80-84. Applying the FISMA/NIST RMF 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; 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:

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

- Module 11: Reciprocity

Lunarline's FISMA/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

85. Applying the FISMA/NIST RMF Intensity 4 Day

Federal Information Security Management Act

Overview: Lunarline's Federal Information Security Management Act (FISMA)/NIST 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 hands-on 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. The fourth day of the FISMA/NIST RMF Intensity course provides each student with a hands-on experience in using automated vulnerability assessment and other tools used to support the Federal authorization process.

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:

- Module 1: Critical Definitions and Policies
- Module 2: C&A Transformation/Transition Overview
- Module 3: The IC and the Transformation
- Module 4: Roles and Responsibilities
- Module 5: Accreditation Boundary
- Module 6: System Categorization
- Module 7: Select Security Controls
- Module 8: Implement, Document & Assess Security Controls
- Module 9: Authorize Information System
- Module 10: Monitor Information System
- Module 11: Reciprocity
- Module 12: Supporting Tools
- Module 13: Certification Testing

Lunarline's FISMA/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's FISMA/NIST RMF Intensity 4 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 and CNSSI 4012 Certificate for successful participation in the course, which will allow students to add the (CNSS) NSTISSI 4011 and CNSSI 4012 designation to their resumes.

86-90. Applying the FISMA/NIST RMF / 800-53 Security Controls Validator 5 Day *Federal Information Security Management Act*

Prerequisite/Who Should Attend: Students should have a fundamental knowledge of the requirements for conducting independent validation assessments, annual assessments, and audits using NIST SP 800-53A and NIST SP 800-115. Although this course does provide an introduction on the Risk Management Framework (RMF), this course concentrates specifically on the testing of the 18 families of controls.

Overview: 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 FISMA/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's Applying the FISMA/NIST Risk Management Framework / 800-53 Security Controls Validator 5 Day course will receive a National Security Agency (NSA)/Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow students to add the NSA/CNSS 4011 designation to their resumes.

91-95. Applying the CNSS/NIST RMF 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:

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

Lunarline's CNSS/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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.

96. Applying the CNSS/NIST RMF Intensity 4 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 using the CNSS and IC requirements 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, and CNSS 1253.

The fourth day of the CNSS/NIST RMF Intensity course provides each student with a hands-on experience in using automated vulnerability assessment and other tools used to support the Federal and CNSS system authorization process.

Modules:

- Module 1: Critical Definitions and Policies
- Module 2: C&A Transformation/Transition Overview
- Module 3: The IC and the Transformation
- Module 4: Roles & Responsibilities
- Module 5: Accreditation Boundary
- Module 6: System Categorization
- Module 7: Select Security Controls
- Module 8: Implement, Document & Assess Security Controls
- Module 9: Authorize Information System
- Module 10: Monitor Information System
- Module 11: Reciprocity
- Module 12: Supporting Tools and Testing
- Module 13: Certification Testing

Lunarline's CNSS/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's CNSS/NIST RMF Intensity 4 Day course will receive a National Security Agency (NSA) and Committee on National Security Systems (CNSS) NSTISSI 4011 and CNSSI 4012 Certificate for successful participation in the course, which will allow students to add the (CNSS) NSTISSI 4011 and CNSSI 4012 designation to their resumes.

97-101. Applying the CNSS/NIST RMF / 800-53 Security Controls Validator 5 Day *Certified Committee on National Security Systems*

Overview: 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 CNSS/NIST 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 CNSS/NIST Classes Include the Following Takeaway Items: A printed training manual, a CD with a comprehensive set of NIST-Director of National Intelligence (DNI) approved templates, as well as copies of the guidelines, instructions, standards, and presentations discussed during the training. The student 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 Lunarline's Applying the CNSS/NIST Risk Management Framework / 800-53 Security Controls Validator 5 Day course will receive a National Security Agency (NSA)/Committee on National Security Systems (CNSS) NSTISSI 4011 Certificate for successful participation in the course, which will allow students to add the NSA/CNSS 4011 designation to their resumes.

Terms and Conditions Applicable to Information Technology (IT) Professional Services (SIN 132-51)

1. Scope

- a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT Professional Services within the scope of this Information Technology Schedule.
- b. The Contractor shall provide services at the Contractor's facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. Performance Incentives I-FSS-60 Performance Incentives (Apr 2000)

- a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or BPAs under this contract.
- b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or BPAs.
- c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. Order

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

4. Performance of Services

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

5. Stop-Work Order (FAR 52.242-15) (Aug 1989)

- a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either:
 - i. Cancel the stop-work order; or
 - ii. Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.
- b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if:
 - i. The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
 - ii. The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.
- c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.
- d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. Inspection of Services

In accordance with FAR 52.212-4 Contract Terms and Conditions – Commercial Items (MAR 2009) (Deviation I - FEB 2007) for Firm-Fixed Price orders and FAR 52.212-4 Contract Terms and Conditions – Commercial Items (MAR 2009) (Alternate I - OCT 2008) (Deviation I – FEB 2007) applies to Time-and-Materials and Labor-Hour Contracts orders placed under this contract.

7. Responsibilities of the Contractor

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8. Responsibilities of the Ordering Activity

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

9. Independent Contractor

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

10. Organizational Conflicts of Interest

a. Definitions.

- i. “Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.
- ii. “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.
- iii. An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

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

11. Invoices

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

12. Payments

For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (Alternate I – OCT 2008) (Deviation I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (Alternate I – OCT 2008) (Deviation I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31(Feb 2007) Time-and-Materials/Labor-Hour Proposal

Requirements - Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

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

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

13. 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.

14. Description of IT Professional Services and Pricing

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

**Terms and Conditions Applicable to Purchase of
Training Courses for General Purpose Commercial
Information Technology Equipment and Software (SIN 132-50)**

1. Scope

- a. The Contractor shall provide training courses normally available to commercial customers, which will permit ordering activity users to make full, efficient use of general purpose commercial IT products. Training is restricted to training courses for those products within the scope of this solicitation.
- b. The Contractor shall provide training at the Contractor's facility and/or at the ordering activity's location, as agreed to by the Contractor and the ordering activity.

2. Order

Written orders, EDI orders (GSA Advantage! And FACNET), credit card orders, and orders placed under BPAs shall be the basis for the purchase of training courses in accordance with the terms of this contract. Orders shall include the student's name, course title, course date and time, and contracted dollar amount of the course.

3. Time of Delivery

The Contractor shall conduct training on the date (time, day, month, and year) agreed to by the Contractor and the ordering activity.

4. Cancellation and Rescheduling

- a. The ordering activity will notify the Contractor at least seventy-two (72) hours before the scheduled training date if a student will be unable to attend. The Contractor will then permit the ordering activity to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the ordering activity will modify its original training order to specify the time and date of the rescheduled training class.
- b. In the event the ordering activity fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the ordering activity will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the ordering activity to reschedule a student who fails to attend a training class within ninety (90) days from the original course date, at no additional charge.
- c. The ordering activity reserves the right to substitute one student for another up to the first day of class.
- d. In the event the Contractor is unable to conduct training on the date agreed to by the Contractor and the ordering activity, the Contractor must notify the ordering activity at least seventy-two (72) hours before the scheduled training date.

5. Follow-Up Support

The Contractor agrees to provide each student with unlimited telephone support or online support for a period of one (1) year from the completion of the training course. During this period, the student may contact the Contractor's instructors for refresher assistance and answers to related course curriculum questions.

6. Price for Training

The price that the ordering activity will be charged will be the ordering activity training price in effect at the time of order placement, or the ordering activity price in effect at the time the training course is conducted, whichever is less.

7. Invoices and Payment

Invoices for training shall be submitted by the Contractor after ordering activity completion of the training course. Charges for training must be paid in arrears (31 U.S.C. 3324). Prompt payment discount, if applicable, shall be shown on the invoice.

8. Format and Content of Training

- a. The Contractor shall provide written materials (i.e., manuals, handbooks, texts, etc.) normally provided with course offerings. Such documentation will become the property of the student upon completion of the training class.
- b. For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.
- c. The Contractor shall provide each student with a Certificate of Training at the completion of each training course.
- d. The Contractor shall provide the following information for each training course offered:
 - i. The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);
 - ii. The length of the course;
 - iii. Mandatory and desirable prerequisites for student enrollment;
 - iv. The minimum and maximum number of students per class;
 - v. The locations where the course is offered;
 - vi. Class schedules; and
 - vii. Price (per student, per class (if applicable)).
- e. For those courses conducted at the ordering activity’s location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on order placed under the MAS, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts. The Industrial Funding Fee does NOT apply to travel and per diem charges.
- f. For online training courses, a copy of all training material must be available for electronic download by the students.

9. “No Charge” Training

The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below.
