
Authorized Federal Supply Service
Information Technology Schedule Pricelist
General Purpose Commercial Information Technology
Equipment, Software and Services

FSC Group 70, SIN 132-50

**TRAINING COURSES FOR INFORMATION TECHNOLOGY
EQUIPMENT AND SOFTWARE**

FSC Group 70, SIN 132-51

INFORMATION TECHNOLOGY PROFESSIONAL SERVICES

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

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

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

SECURE | IT

SECUREIT CONSULTING GROUP, INC.

1902 CAMPUS COMMONS DRIVE • RESTON, VIRGINIA 20191

Telephone: (703) 230-0734 • Fax: (703) 464-5990 • Internet: www.secureit.com

Contract Number: **GS-35F-0644N**

Contract Period: 12/27/08 to 5/27/13

Pricelist current through Contract Renewal and Modification Number: PO-0011

General Services Administration
Federal Supply Service

Products and ordering information in this Authorized FSS Information Technology Schedule Pricelist are also available on the GSA Advantage! System. Agencies can browse GSA Advantage! by accessing the home Page via the Internet at [http:// www.gsaadvantage.gov](http://www.gsaadvantage.gov) /

Table of Contents

Information for Ordering Offices	1
Special Notice to Agencies	1
1. Geographic Scope of Contract	1
2. Contractor’s Ordering Address and Payment Information	1
3. Liability for Injury or Damage	2
4. Statistical Data for Government Ordering Office Completion of Standard Form 279.....	3
5. FOB	3
6. Delivery Schedule.....	3
7. Discounts.....	3
8. Trade Agreements Act of 1979, As Amended	4
9. Statement Concerning Availability of Export Packing	4
10. Small Requirements	4
11. Maximum Order	4
12. Use of Federal Supply Service Information Technology Schedule Contracts.....	4
13. Federal Information Technology / Telecommunications Standards Requirements	6
13.1 Federal Information Processing Standards Publications (FIPS PUBS).....	6
13.2 Federal Telecommunications Standards (FED-STDS)	6
14. Contractor Tasks / Special Requirements.....	7
15. Contract Administration for Ordering Offices	7
16. GSA Advantage!.....	8
17. Purchase of Open Market Items	8
18. Contractor Commitments, Warranties, and Representations.....	8
19. Overseas Activities	9
20. Blanket Purchase Agreements (BPAs).....	9
21. Contractor Team Arrangements	9
22. Installation, Deinstallation, Reinstallation.....	9
23. Section 508 Compliance.....	10
24. Prime Contractor Ordering From Federal Supply Schedules.....	10
25. Insurance – Work on a Government Installation.....	10
 Terms and Conditions Applicable to Training Courses (SIN 132-50) for General Purpose Commercial Information Technology Equipment and Software	 12
1. Scope	12
2. Order	12
3. Time of Delivery.....	12
4. Cancellation and Rescheduling	12

5. Follow-Up Support 13
 6. Price for Training 13
 7. Invoices and Payment 13
 8. Format and Content of Training 13
 9. Course Descriptions 14
 10. Course Schedule and Locations 36
 11. Table of Prices 36

Terms and Conditions Applicable to Information Technology Professional Services (SIN 132-51) for General Purpose Commercial Information Technology Services 38

1. Scope 38
 2. Performance Incentives 38
 3. Ordering Procedures for Services 38
 4. Order 41
 5. Performance of Services 41
 6. Stop-Work Order 42
 7. Inspection of Services 42
 8. Responsibilities of Contractor 42
 9. Responsibilities of the Ordering Activity 42
 10. Independent Contractor 43
 11. Organizational Conflicts of Interest 43
 12. Invoices 43
 13. Payments 43
 14. Résumés 43
 15. Incidental Support Costs 44
 16. Approval of Subcontracts 44
 17. Description of IT Services and Pricing 44
 17.1 IT Professional Services 44
 17.2 Commercial Job Titles (Labor Categories) 47
 17.3 Prices for IT Professional Services at Hourly Rates 54
 USA Commitment to Promote Small Business Participation Procurement Programs 56
 Suggested Blanket Purchase Agreement (BPA) 57
 Basic Guidelines for Using “Contractor Team Arrangements” 59

Information for Ordering Activities Applicable to All Special Item Numbers

SPECIAL NOTICE TO AGENCIES: Small Business Participation

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

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

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

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

1. GEOGRAPHIC SCOPE OF CONTRACT

48 contiguous States, including D.C, Alaska, Hawaii, and Puerto Rico

2. CONTRACTOR'S ORDERING ADDRESS AND PAYMENT INFORMATION

Ordering Information:

SecureIT Consulting Group, Inc. is doing business as SecureIT.

- a. The following representatives should be contacted for ordering information:

Jim Graham
Senior VP, Federal Programs and GSA Schedule Program Manager
SecureIT
1902 Campus Commons Drive, Suite 100
Reston, Virginia 20191
Direct: (703) 230-0734 Main: (703) 464-7010
e-mail: jgraham@secureit.com

David Trout
President
SecureIT
1902 Campus Commons Drive, Suite 100
Reston, Virginia 20191
(703) 464-7010
e-mail: dtroat@secureit.com

b. Address mailed orders as follows:

SecureIT
Attn: Jim Graham
GSA Schedule Program Manager
1902 Campus Commons Drive, Suite 100
Reston, Virginia 20191

Payment Address:

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

Payment Via Check/U.S. Mail:
SecureIT, Inc.
1902 Campus Commons Drive, Suite 100
Reston, Virginia 20191

The following telephone numbers can be used by ordering activities to obtain technical and/or ordering assistance.

Technical: Jim Graham, (703) 230-0734, jgraham@secureit.com

Ordering: Jim Graham, (703) 230-0734, jgraham@secureit.com

Payment: Keli Winter, (703) 464-7010, kwinter@secureit.com

Alternate: David Trout, 703-464-7010, dtroat@secureit.com

3. LIABILITY FOR INJURY OR DAMAGE

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

8. TRADE AGREEMENTS ACT OF 1979, AS AMENDED:

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

9. STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING

Not Applicable.

10. SMALL REQUIREMENTS

The minimum dollar value of orders to be issued is \$100.

11. MAXIMUM ORDER

SIN 132-50 – Training Courses	\$25,000 per order
SIN 132-51 - Information Technology (IT) Professional Services	\$500,000 per order

12. USE OF FEDERAL SUPPLY SERVICE INFORMATION TECHNOLOGY SCHEDULE CONTRACTS.

In accordance with FAR 8.404. Special ordering procedures have been established for each SIN. Refer to the applicable Terms and Conditions sections following in this Pricelist.

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

- a. Orders placed at or below the micro-purchase threshold. Ordering activities can place orders at or below the micro-purchase threshold with any Federal Supply Schedule Contractor.
- b. Orders exceeding the micro-purchase threshold but not exceeding the maximum order threshold. Orders should be placed with the Schedule Contractor that can provide the supply or service that represents the best value. Before placing an order, ordering activities should consider reasonably available information about the supply or service offered under MAS contracts by using the “GSA Advantage!” on-line shopping service, or by reviewing the catalogs/pricelists of at least three Schedule Contractors and selecting the delivery and other options available under the schedule that meets the ordering activity’s needs. In selecting the supply or service representing the best value, the ordering activity may consider--

- (1) Special features of the supply or service that are required in effective program performance and that are not provided by a comparable supply or service;
- (2) Trade-in considerations;
- (3) Probable life of the item selected as compared with that of a comparable item;
- (4) Warranty considerations;
- (5) Maintenance availability;
- (6) Past performance; and
- (7) Environmental and energy efficiency considerations.

c. Orders exceeding the maximum order threshold. Each schedule contract has an established maximum order threshold. This threshold represents the point where it is advantageous for the ordering activity to seek a price reduction. In addition to following the procedures in paragraph b, above, and before placing an order that exceeds the maximum order threshold, ordering activities shall-

Review additional Schedule Contractors'

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

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

- (1) Offer a new lower price for this requirement (the Price Reductions clause is not applicable to orders placed over the maximum order in FAR 52.216-19 Order Limitations);
- (2) Offer the lowest price available under the contract; or
- (3) Decline the order (orders must be returned in accordance with FAR 52.216-19).

d. Blanket purchase agreements (BPAs). The establishment of Federal Supply Schedule BPAs is permitted when following the ordering procedures in FAR 8.404. All schedule contracts contain BPA provisions. Ordering activities may use BPAs to establish accounts with Contractors to fill recurring requirements. BPAs should address the frequency of ordering and invoicing, discounts, and delivery locations and times.

e. Price reductions. In addition to the circumstances outlined in paragraph c, above, there may be instances when ordering activities will find it advantageous to request a price reduction. For example, when the ordering activity finds a schedule supply or service elsewhere at a lower price or when a BPA is being established to fill recurring requirements, requesting a price reduction could be advantageous. The potential volume of orders under these agreements, regardless of the size of the individual order, may offer the ordering activity the opportunity to secure greater discounts. Schedule Contractors are not required to pass on to all schedule users a price reduction extended only to an individual ordering activity for a specific order.

f. Small business. For orders exceeding the micro-purchase threshold, ordering activities should give preference to the items of small business concerns when two or more items at the same delivered price will satisfy the requirement.

g. Documentation. Orders should be documented, at a minimum, by identifying the Contractor the item was purchased from, the item purchased, and the amount paid. If an ordering activity requirement in excess of the micro-purchase threshold is defined so as to require a particular brand name, product, or feature of a product peculiar to one manufacturer, thereby precluding consideration of a product manufactured by another company, the ordering activity shall include an explanation in the file as to why the particular brand name, product, or feature is essential to satisfy the ordering activity's needs.

13. FEDERAL INFORMATION TECHNOLOGY / TELECOMMUNICATION STANDARDS REQUIREMENTS

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

13.1 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS)

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

13.2 FEDERAL TELECOMMUNICATION STANDARDS (FED-STDS)

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

14. CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2001)

Telephone: (703) 230-0734 • Fax: (703) 464-5990 • www.secureit.com

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

15. CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES

Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under

provisions of FAR 52.249-1, 52.249-2, and 52.249-8, paragraphs (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See C.1.)

16. GSA ADVANTAGE!

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

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

Agencies can browse *GSA Advantage!* by accessing the Internet World Wide Web utilizing a browser (e.g., NETSCAPE). The Internet address is [http:// www.gsaadvantage.gov/](http://www.gsaadvantage.gov/).

17. PURCHASE OF OPEN MARKET ITEMS

NOTE: Open Market Items are also known as incidental items, non-contract items, non-Schedule items, and items not on a Federal Supply Schedule contract. ODCs (Other Direct Costs) are not part of this contract and should be treated at open market purchases. Ordering Activities procuring open market items must follow FAR 8.401(d).

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

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

18. CONTRACTOR COMMITMENTS, WARRANTIES, AND REPRESENTATIONS

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

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

19. OVERSEAS ACTIVITIES

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

None.

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

20. BLANKET PURCHASE AGREEMENTS (BPAs)

Federal Acquisition Regulation (FAR) 13.201(a) defines Blanket Purchase Agreements (BPAs) as "...a simplified method of filling anticipated repetitive needs for supplies or services by establishing 'charge accounts' with qualified sources of supply." The use of Blanket Purchase Agreements under the Federal Supply Schedule Program is authorized in accordance with FAR 13.202(c)(3), which reads, in part, as follows:

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

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

21. CONTRACTOR TEAM ARRANGEMENTS

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Contractor's Reports of Sales and 552.238-76, Industrial Funding Fee, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

22. INSTALLATION, DEINSTALLATION, REINSTALLATION

The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of \$2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair

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

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

23. SECTION 508 COMPLIANCE

If applicable, Section 508 compliance information on the services in this contract are available in Electronic and Information Technology (EIT) at the following: **www.secureit.com**. The EIT standard can be found at: www.Section508.gov/.

24. PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES

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

- (a) A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and
- (b) The following statement:
This order is placed under written authorization from _____ dated _____. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

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

- (a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.
- (b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—
 - (1) For such period as the laws of the State in which this contract is to be performed prescribe; or
 - (2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

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

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 blanket purchase agreements (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 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. See listings at paragraphs 10. & 11. below for training course information and prices.

e. For those courses conducted at the ordering activity's location, instructor travel charges (if applicable), including mileage and daily living expenses, must be indicated below. Rates paid as a result of travel must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts.

We will charge for required travel in accordance with Federal Travel Regulation/ Joint Travel Regulations per diem and mileage rates in effect on the dates training at an ordering activity site is required.

9. COURSE DESCRIPTIONS

All available “off-the-shelf” courses (i.e., seminars) are described below. Customized courses can be developed, but are outside the scope of this Schedule contract. Additional information regarding “off-the-shelf” courses can be found at www.secureit.com.

Course: INTRODUCTION TO IT AUDITING**Overview:**

This seminar will give participants the knowledge necessary to understand and effectively evaluate controls in an information processing environment. It will outline and define basic technical concepts, and provide a risk-based approach for ensuring that adequate controls have been implemented. The seminar will incorporate guidance contained in leading industry standards, most notably the Control Objectives for Information Technology (COBIT) and the Federal Information Systems Controls Audit Manual (FISCAM). It will begin at a very basic level and slowly progress into more complex technology issues that are prevalent in today's information processing environments. The course will consist of modules that address the core areas of IT risk. Each module will explain the objectives, risks, key controls, and primary audit procedures that can be used. You will leave this seminar with a solid knowledge of key technology concepts, and the foundation needed to audit these technologies and processes effectively.

Audience:

This course is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- ❑ Information Technology Risk
- ❑ Categories of Risks and Controls
- ❑ IT Control Environment
- ❑ Security Management
- ❑ Operating Systems Security Management
- ❑ Network Security Management
- ❑ Electronic Communications
- ❑ Disaster Recovery & Business Continuity
- ❑ Systems Management
- ❑ Physical, Environmental, & Operations Management
- ❑ Database Management
- ❑ Change Management
- ❑ Systems Development
- ❑ Application Controls
- ❑ Types of Audits

Course Duration:

2 days (14 CPEs)

Course Name: IT AUDIT BOOTCAMP**Overview:**

This seminar will give participants the knowledge necessary to understand and effectively evaluate both general and application controls in an information processing environment. It will outline and define basic technical concepts, incorporate concepts for modern web and distributed applications, and provide a risk-based approach for ensuring that adequate controls have been implemented. The seminar will incorporate guidance contained in leading industry standards, most notably the Control Objectives for Information Technology (COBIT) and the Federal Information Systems Controls Audit Manual (FISCAM). It will begin at a very basic level and slowly progress into more complex technology issues that are prevalent in today's information processing environments. The course will consist of modules that address the core areas of IT risk. Each module will explain the objectives, risks, key controls, and primary audit procedures that can be used. You will leave this seminar with a solid knowledge of key technology concepts, and the foundation needed to audit these technologies and processes effectively.

Audience:

This course is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- ❑ Information Technology Risk
- ❑ Categories of Risks and Controls
- ❑ IT Control Environment
- ❑ Security Management
- ❑ Operating Systems Security Management
- ❑ Network Security Management
- ❑ Electronic Communications
- ❑ Disaster Recovery & Business Continuity
- ❑ Systems Management
- ❑ Physical, Environmental, & Operations Management
- ❑ Database Management
- ❑ Change Management
- ❑ Systems Development
- ❑ Transactional Integrity, Consistency, Accuracy, Validity
- ❑ Application-level Security
- ❑ Application Controls: Integration with General Controls
- ❑ Types of Audits

Course Duration:

3 days (21 CPEs)

Course Name: AUDITING CISCO ROUTERS**Overview:**

With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. They must also rely on other network security components to provide this protection, including firewalls, intrusion detection systems, and routers. These components must be properly configured to ensure that only authorized network traffic is able to pass through to internal networks. This technical seminar will give participants the knowledge necessary to thoroughly understand and effectively evaluate the configuration of a Cisco router, and case studies will reinforce important concepts learned. It will also help participants understand the various components of a Cisco router, and give them the tools needed to effectively audit their configurations.

Audience:

This course is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Introduction to Routers
- ❑ Routers & Network Security
- ❑ TCP/IP Internetworking
- ❑ Network Interfaces & Routes
- ❑ Basic Access Lists
- ❑ Advanced Access Lists
- ❑ Hardening Router IOS & Services
- ❑ Terminal Line Authentication & Access Controls
- ❑ Security Servers & Cisco AAA
- ❑ Logging & Monitoring
- ❑ Change & Systems Management
- ❑ Router Advanced Features
- ❑ An Approach for Auditing Cisco Routers
- ❑ Cisco Router Case Study

Course Duration:

2 days (14 CPEs)

Course Name: AUDITING CISCO ROUTERS: THE ESSENTIALS**Overview:**

With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. They must also rely on other network security components to provide this protection, including firewalls, intrusion detection systems, and routers. These components must be properly configured to ensure that only authorized network traffic is able to pass through to internal networks. This technical seminar will give participants the knowledge necessary to understand and effectively evaluate the configuration of a Cisco router. It will help participants understand the various components of a Cisco router, and give them the tools needed to effectively audit their configurations.

Audience:

This course is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Introduction to Routers & Network Security
- ❑ Network Interfaces & Routes
- ❑ Basic Access Lists
- ❑ Hardening Router IOS & Services
- ❑ Terminal Line Authentication & Access Controls
- ❑ Logging & Monitoring
- ❑ An Approach for Auditing Cisco Routers

Course Duration:

1 days (7 CPEs)

Course Name: AUDITING FIREWALLS**Overview:**

With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. Firewalls have emerged as the primary tools used to prevent unauthorized access. Firewalls are placed at the logical borders of an enterprise and aim to prevent unauthorized access to or from the private network. Considering how important these protection mechanisms are, organizations need to ensure not only that they are strategically placed, but also that they are configured in a secure manner. This course will give participants the knowledge necessary to understand and effectively evaluate the configuration of a firewall. Two of the industry's leading firewalls will be discussed in depth and case studies will reinforce important concepts learned. This course will help participants understand the various firewall technologies and give them the tools needed to effectively audit them.

Audience:

This course is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Network Security Basics
- ❑ TCP/IP Internetworking
- ❑ Firewall Topologies & Architectures
- ❑ Hardening the Host
- ❑ Firewall Filtering
- ❑ Firewall Administration & Management
- ❑ Network Security Monitoring
- ❑ Logging & Monitoring
- ❑ NAT & VPN
- ❑ CERT Evaluative Criteria
- ❑ Auditing Checkpoint Firewall-1
- ❑ Case Study: Checkpoint Firewall-1
- ❑ Auditing Symantec Raptor Firewall

Course Duration:

2 days (14 CPEs)

Course Name: AUDITING FIREWALLS: THE ESSENTIALS**Overview:**

With increased connectivity to the Internet, organizations can no longer simply rely on operating system security to protect their valuable corporate data. Firewalls have emerged as the primary tools used to prevent unauthorized access. Firewalls are placed at the logical borders of an enterprise and aim to prevent unauthorized access to or from the private network. Considering how important these protection mechanisms are, organizations need to ensure not only that they are strategically placed, but also that they are configured in a secure manner. This course will give participants the knowledge necessary to understand and effectively evaluate the configuration of a firewall. It will help attendees understand the various firewall technologies, and give them the tools needed to effectively audit them.

Audience:

This course is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Network Security Basics
- ❑ Firewall Topologies & Architectures
- ❑ Hardening the Host
- ❑ Firewall Filtering – Theory
- ❑ Firewall Filtering - Practice
- ❑ Firewall Administration & Management
- ❑ Network Security Monitoring
- ❑ Logging & Monitoring

Course Duration:

1 day (7 CPEs)

Course Name: AUDITING CHECKPOINT FIREWALL-1**Overview:**

Firewalls have emerged as the primary tools used to prevent unauthorized access. Firewalls are placed at the logical borders of an enterprise and aim to prevent unauthorized access to or from the private network. Considering how important these protection mechanisms are, organizations need to ensure not only that they are strategically placed, but also that they are configured in a secure manner. This course will give participants the knowledge necessary to understand and effectively evaluate the configuration of a Checkpoint Firewall-1 firewall, and a hands-on case study will reinforce important concepts learned. Topics covered in this course will include: administration, security policy and objects, interfaces, properties, rules, state tracking, logging and alerting, authentication, security servers, network address translation, virtual private networks, and overall monitoring.

Audience:

This course is targeted towards mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Introduction to Network Security & Firewalls
- ❑ Filtering, Administrative Access, Logging & Monitoring
- ❑ Hardening the Host
- ❑ Checkpoint Firewall-1
 - Administration
 - Firewall-1 Security Policy and Objects
 - Interfaces – Spoofing settings
 - Properties
 - Rules
 - State Tracking
 - Logging and Alerting
 - Authentication
 - Security Servers
 - Network Address Translation
 - Virtual Private Networks
 - Overall Monitoring

Course Duration:

1 day (7 CPEs)

Course Name: AUDITING NETWORK SECURITY: THE BASICS**Overview:**

Organizations can no longer simply rely on operating system security to protect their valuable corporate data. They must also rely on network security components to provide this protection, including firewalls, intrusion detection systems, and routers. These components must be properly configured to ensure that only authorized network traffic is able to pass through to internal networks. This course will help you understand the basics of each of these components, along with the role each plays in the overall network security architecture.

Audience:

This course is targeted for mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing and monitoring the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Network Security Fundamentals
- ❑ Network Security Policy
- ❑ Firewall Topologies & Architectures
- ❑ Cryptography
- ❑ Intrusion Detection Systems
- ❑ Introduction to Routers
- ❑ Network Security Monitoring

Course Duration:

1 day (7 CPEs)

Course Name: NETWORK SECURITY BOOTCAMP FOR IT AUDITORS**Overview:**

Organizations can no longer rely on operating system security to protect their valuable corporate data. They must also rely on network security components to provide this protection, including firewalls, routers, VPNs, and intrusion detection systems. These components must be properly configured to ensure that only authorized traffic is able to pass through to internal networks. This course will help attendees understand and effectively evaluate the configuration of a firewall, the various components of a Cisco router, the mechanics of encryption and IPSec VPNs, and the different types of intrusion detection systems. This course, designed specifically for IT Auditors and IT Security professionals, will provide the tools and techniques needed to effectively audit these network security components and determine their effectiveness in an organization's overall security strategy.

Audience:

This course is targeted for mid to senior level auditors, system administrators, Information Technology personnel, and all other security professionals tasked with securing and monitoring the borders of their enterprises.

Prerequisites:

An understanding of basic networking concepts and technologies

Outline:

- ❑ Network Security Basics
- ❑ TCP/IP Internetworking
- ❑ Network Security Policy
- ❑ Firewall Topologies & Architectures
- ❑ Hardening the Host
- ❑ Firewall Filtering
- ❑ Firewall Administration & Management
- ❑ Network Security Monitoring
- ❑ Logging & Monitoring
- ❑ NAT & VPN
- ❑ Auditing Checkpoint Firewall-1
- ❑ IPSec VPN
- ❑ Cryptography
- ❑ Introduction to IDS
- ❑ IDS Architecture
- ❑ IDS- What to Monitor
- ❑ IDS Maintenance
- ❑ Intrusion Response Planning
- ❑ Introduction to Routers
- ❑ Routers & Network Security
- ❑ Network Interfaces & Routes

- ❑ Basic Access Lists
- ❑ Advanced Access Lists
- ❑ Hardening Router IOS & Services
- ❑ Terminal Line Authentication & Access Controls
- ❑ Security Servers & Cisco AAA
- ❑ Logging & Monitoring
- ❑ Change & Systems Management
- ❑ Router Advanced Features
- ❑ An Approach for Auditing Cisco Routers
- ❑ Network Security Monitoring

Course Duration:

5 days (35 CPEs)

Course Name: AUDITING DISTRIBUTED & WEB-BASED APPLICATIONS**Overview:**

This course, designed specifically for government and private-sector IT Auditors, will provide the tools and techniques needed to effectively understand and audit modern distributed and web-based applications. The control techniques that are used to address risk in distributed and web-based systems are substantially different from the traditional techniques used in legacy mainframe environments. Unlike many generic Application Auditing courses, this course will focus specifically on distributed system control techniques and the unique risks of the supporting technologies. This course addresses infrastructure controls (network security, electronic communications, etc.) as well as application and middleware controls (transactional integrity, application recoverability, etc.) that protect the reliability and integrity of critical data. Every module of this course will outline “best practice” control techniques and include suggested audit procedures. The course incorporates standard auditing control objectives such as GAO’s FISCAM, ISACA’s COBIT, and ISACF’s Objectives for NetCentric Technology. The lectures and course materials will complement these established guidelines by providing practical steps for performing effective audits of modern network-based and web applications.

Audience:

IT Audit professionals, and others tasked with evaluating controls over modern distributed and web-based applications.

Prerequisites:

None

Outline:

- ❑ Information Technology Risk
- ❑ Auditing Systems Management
- ❑ Auditing Change Management
- ❑ Auditing Electronic Communications
- ❑ Auditing Network Security Management
- ❑ Auditing Encryption & VPNs
- ❑ Auditing Operating System Security
- ❑ Auditing Database Management
- ❑ Auditing Data Management
- ❑ Application Security Architectures
- ❑ Auditing Application Security Management
- ❑ Auditing Data Accuracy & Validation
- ❑ Auditing Input/Output Controls
- ❑ Auditing Balancing & File Version Controls
- ❑ Auditing Transactional Integrity
- ❑ Auditing Tuxedo
- ❑ Auditing Application Recoverability
- ❑ Auditing Web-based Applications
- ❑ Auditing Object-Oriented and Java Applications

Course Duration:

3 days (21 CPEs)

Course Name: AUDITING SOLARIS**Overview:**

Hardening the operating system is the first, and one of the most fundamental, steps in ensuring that mission critical information is adequately protected on Corporate systems. After an explanation of the key concepts and components of the UNIX operating system, the seminar will outline common UNIX vulnerabilities, threats, and exploits used by hackers to obtain unauthorized access to UNIX-based networks. The seminar will be focused on Sun Solaris, as this flavor of UNIX clearly dominates the market and would be the version most often encountered by an IT Auditor. The seminar focuses on “general purpose” Solaris configuration issues, with only a brief discussion of Solaris 8 specific configurations that are not yet widely used. Finally, the seminar will identify and discuss specific audit procedures for reviewing and evaluating the security of Sun Solaris UNIX installations.

Audience:

IT Audit professionals, and others tasked with evaluating controls over UNIX-based systems.

Prerequisites:

A basic understanding of UNIX and general IT concepts

Outline:

- ❑ Users/groups/root/password file
- ❑ Authentication/shadow file/NIS
- ❑ File Permissions/setUID/UNIX file system
- ❑ System startup and user initialization files
- ❑ Cron and At
- ❑ Network services/Inetd.conf
- ❑ Networking: trusted hosts and users/RPC/NFS
- ❑ UNIX event logging/syslog/loginlog
- ❑ Other UNIX configurations: routing/eprom password/buffer overflows

Course Duration:

2 days (14 CPEs)

Course Name: AUDITING WINDOWS AND IIS**Overview:**

This seminar will give participants the knowledge necessary to understand and effectively evaluate controls over web servers running Microsoft’s Internet Information Server (IIS) on the Windows server platform. Security controls will be the primary focus of the course. The course will address general principles and concepts, as well as the detailed technical implementations and configuration settings related to securing and controlling a Microsoft web server. The course will also provide “how to” instruction on accessing the control-related settings, files, and other information required to perform an effective risk assessment. The course will address the following topic areas: network architectures for web servers, hardening Windows, web server security policies and access control, IIS security properties, Windows server and IIS server filtering, logging and auditing options, SSL settings for confidentiality, and IIS-related web content issues.

Audience:

IT Audit professionals, and others tasked with evaluating controls over Windows IIS servers.

Prerequisites:

A basic understanding of Windows and general IT concepts

Outline:

- ❑ Web Technology
- ❑ Hardening Principles
- ❑ Secure Network Architectures for the Web
- ❑ Service Minimization and Patching
- ❑ Security Policies
- ❑ Audit Policies and Logging
- ❑ Other Hardening Controls
- ❑ Filtering Traffic on Windows Servers
- ❑ Windows Secure Remote Administration
- ❑ Introduction to IIS
- ❑ IIS Service Manager Security Settings
- ❑ IIS Security
- ❑ Hardening Tools
- ❑ Securing Active Content
- ❑ IIS Logging

Course Duration:

2 days (14 CPEs)

Course Name: AUDITING WINDOWS**Overview:**

Windows includes a host of security features that dramatically improves the Windows security posture. However, these new features add a level of complexity that needs to be well understood by those responsible for evaluating its effectiveness. This seminar will outline the steps necessary to ensure that Windows servers are configured securely. The course will address general principles and concepts, as well as the detailed technical implementations and configuration settings related to securing and controlling a Microsoft server. The course will also provide “how to” instruction on accessing the control-related settings, files, and other information required to perform an effective risk assessment.

Audience:

IT Audit professionals, and others tasked with evaluating controls over Windows IIS servers.

Prerequisites:

A basic understanding of Windows and general IT concepts

Outline:

- ❑ Windows Concepts
- ❑ Controls Over the Administrator Account
- ❑ Authentication and Account Policy
- ❑ Rights and Privileges
- ❑ Privileged Programs
- ❑ Domains and Trust Relationships
- ❑ Active Directory
- ❑ File & Directory Permissions
- ❑ Registry Key Values & Permissions
- ❑ File Sharing
- ❑ Security Tools
- ❑ Logging
- ❑ Service Packs

Course Duration:

3 days (21 CPEs)

Course Name: AUDITING ORACLE DATABASES**Overview:**

This seminar will give participants the knowledge necessary to understand and effectively evaluate controls over an Oracle database management system. Participants will learn the various facilities of Oracle and the controls that provide security, integrity, and recovery controls for the Oracle database and the information contained therein. Areas that will be addressed include security architecture, user authentication controls, discretionary access controls, privileged access controls, auditing controls, host operating system controls, database object and transactional integrity controls, and database recovery controls. The course will focus on how Oracle databases can be controlled in network-centric and multi-tier distributed application environments.

Audience:

IT Audit professionals, and others tasked with evaluating controls over Oracle database servers.

Prerequisites:

A basic understanding of general IT concepts

Outline:

- ❑ Introduction to Oracle
- ❑ Security Architectures for Distributed Systems
- ❑ Authentication
- ❑ Database Objects
- ❑ User Privileges
- ❑ User Roles
- ❑ Database Application Security Strategy
- ❑ SQL-Plus Security
- ❑ Database Links
- ❑ System Security Infrastructure
- ❑ Logging & Auditing
- ❑ Host-level Security
- ❑ Oracle Advanced Security
- ❑ Database Integrity
- ❑ Transactional Integrity
- ❑ Database Recoverability

Course Duration:

2 days (14 CPEs)

Course Name: FISCAM & COBIT GENERAL CONTROLS AUDITING**Overview:**

This seminar will give participants the knowledge necessary to understand and effectively evaluate both general and application controls in an information processing environment. The seminar will incorporate and be based on guidance contained in leading industry standards, most notably the Control Objectives for Information Technology (COBIT), and the Federal Information Systems Controls Audit Manual (FISCAM). It will begin at a very basic level and slowly progress into more complex technology issues that are prevalent in today's information processing environments. The course will consist of modules that address the core areas of IT risk. Each module will explain the objectives, risks, key controls, and primary audit procedures that can be used. You will leave this seminar with a solid knowledge of key technology concepts, and the foundation needed to audit these technologies and processes effectively.

Audience:

This course is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- ❑ Information Technology Risk
- ❑ Categories of Risks and Controls
- ❑ IT Control Environment
- ❑ Introduction to FISCAM
- ❑ Introduction to COBIT
- ❑ Security Management
- ❑ Operating Systems Security Management
- ❑ Network Security Management
- ❑ Electronic Communications
- ❑ Disaster Recovery & Business Continuity
- ❑ Systems Management
- ❑ Physical, Environmental, & Operations Management
- ❑ Database Management
- ❑ Change Management
- ❑ Systems Development
- ❑ Transactional Integrity, Consistency, Accuracy, Validity
- ❑ Application-level Security
- ❑ Application Controls: Integration with General Controls
- ❑ Types of Audits
- ❑ Conclusion: Role of FISCAM & COBIT

Course Duration:

3 days (21 CPEs)

Course Name: AUDITING WEB SECURITY**Overview:**

Security best-practice organizations such as SANS, Gartner and ICSA have indicated that 60%-70% of successful hacking attempts were web-based hacks over port 80 that exploited insecure applications, scripts, web forms, or web server vulnerabilities. Traditional network-based firewalls are unable to prevent or detect these types of attacks. This seminar will focus on the risks and vulnerabilities of web technologies, as well as the controls needed to mitigate any weaknesses. Topics that will be addresses include authentication options, cookies, and form fields. Although the focus of this seminar is on security, transaction integrity will be addressed to some extent as well.

Audience:

IT Audit professionals, and others tasked with evaluating controls over Web components.

Prerequisites:

A basic understanding of general IT and web technology concepts

Outline:

- ❑ Introduction to Web Technologies
- ❑ Web Server Processes & Configurations
- ❑ Web Sessions & Authentication
- ❑ SSL
- ❑ Web Resource Access Controls
- ❑ Web Application Vulnerabilities
- ❑ J2EE Transaction & Security Model
- ❑ Outbound Web Infrastructure

Course Duration:

2 days (14 CPEs)

Course Name: **FREEMWARE HACKING – (HANDS-ON)**

Overview:

Audience:

IT Audit professionals, Network Administrators, Security Administrators, and others tasked with securing Corporate networks.

Prerequisites:

A basic understanding of general IT and networking concepts

Outline:

- ❑ Introduction to Network Security Vulnerabilities
- ❑ A Strategic Process for Hacking
- ❑ Setting up a Hacking Infrastructure
- ❑ Network Reconnaissance
- ❑ Network Enumeration tools
- ❑ Port Scanning
- ❑ Network Vulnerability Scanners
- ❑ Password Crackers
- ❑ CIS Assessment tools
- ❑ Windows Baseline and Hacking Tools
- ❑ Web Vulnerability Scanners
- ❑ Web Hacking Tools for Form Field and Cookie Manipulation

Course Duration:

2 days (14 CPEs)

Course Name: WIRELESS SECURITY**Overview:**

This comprehensive seminar will provide attendees with a broad understanding of the security issues that plague Personal Digital Assistant (PDA) and wireless technologies. The session will begin with a brief introduction to PDA and wireless technologies, along with a discussion of their recent advancements. We will then explore the many security issues related to PDAs and wireless devices, particularly as they become more prevalent in corporate infrastructures. Most importantly, we will review how your environment may be at risk and how to mitigate those threats. We will also illustrate how to prevent known vulnerabilities from being exploited. Finally, this seminar will explain how to incorporate PDA and wireless security into an Enterprise Security Program using tools, technology, and policies. The seminar participant should expect to gain insight into the state of PDA and wireless security coupled with "real-world" accounts and useful recommendations from the presenters' industry experiences.

Audience:

IT Audit professionals, and others tasked with evaluating controls over wireless networks.

Prerequisites:

A basic understanding of general IT concepts

Outline:

- ❑ Introduction to PDA and Wireless Technologies
- ❑ Security Issues Surrounding PDAs and Other Wireless Devices
- ❑ Mitigating Wireless Security Risks
- ❑ Incorporating PDA and Wireless Security into An Enterprise Security Program
- ❑ Tools and Technology
- ❑ Policies

Course Duration:

1 day (7 CPEs)

Course Name: INTRUSION DETECTION: FROM START TO FINISH**Overview:**

In the security consulting profession, we are continuously tasked with making recommendations about security products. Customers want to know how to make their corporate infrastructure more secure. Years ago, they would ask which firewall to buy, then they wanted a PKI solution, but now it seems that they need to know which intrusion detection system (IDS) to implement. In response to increased market awareness, companies like ISS, Symantec, and CISCO are raking in the revenues for sales of their IDS solutions. Similarly, freeware solutions like Shadow and Snort are experiencing increasingly frequent download requests. Consequently, intrusion detection has become an important component in the Security Officer's toolbox. However, many security experts are still in the dark about IDS, unsure about what IDS tools do, how to use them, or why they must. This seminar will help answer these questions.

Audience:

IT Auditors, Network Administrators, Security Administrators, and those interested in learning the basics of intrusion detection systems

Prerequisites:

A basic understanding of general IT concepts

Outline:

- ❑ Introduction to Intrusion Detection Concepts
- ❑ Network Intrusion Detection Systems
- ❑ Host-based Intrusion Detection Systems
- ❑ Other Intrusion Detection Types
- ❑ Future of Intrusion Detection
- ❑ Industry Observations

Course Duration:

1 day (7 CPEs)

Course Name: ENTITY-WIDE SECURITY PROGRAM PLANNING & MANAGEMENT**Overview:**

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. This seminar starts by explaining these concepts as outlined in GAO's Federal Information System Controls Audit Manual (FISCAM), and continues on to discuss areas that have not yet been included in GAO guidance. For each area, the applicable

Audience:

This course is designed for entry-level IT Auditors, and financial auditors interested in making the move to IT.

Prerequisites:

None

Outline:

- ❑ Information Security Strategy
- ❑ Types of Security Risks
- ❑ Risk Management Concepts
- ❑ Risk Assessment Process
- ❑ Auditing the Risk Assessment Process
- ❑ Security Policy & Standards
- ❑ Hiring, Termination, & Performance Policies
- ❑ Security Program Plan
- ❑ Security Management Structure
- ❑ Security Awareness
- ❑ Security Monitoring & Evaluation
- ❑ Security Incidents
- ❑ Incident Response
- ❑ Contractual Monitoring & Review

Course Duration:

2 days (14 CPEs)

10. COURSE SCHEDULE AND LOCATIONS

SecureIT offers its training seminars in two venues:

1. On-site at Government sites (under contractual arrangement)
2. Off-site at public locations (open enrollment)

The current schedule of public training course offerings, locations, presentation dates, and electronic registration form can be found at www.secureit.com.

11. TABLE OF TRAINING SEMINAR PRICES

GOVERNMENT SITE PRESENTATIONS			
“OFF-THE-SHELF” SEMINAR TITLE	UP TO 20 ATTENDEES	UP TO 30 ATTENDEES	UP TO 50 ATTENDEES
Introduction to IT Auditing	\$8,150	\$11,415	\$17,667
IT Audit Bootcamp	\$11,894	\$16,652	\$25,771
Auditing CISCO Routers	\$ 9,650	\$13,510	\$20,909
Auditing CISCO Routers: The Essentials	\$5,162	\$7,226	\$11,184
Auditing Firewalls	\$ 9,650	\$13,510	\$20,909
Auditing Firewalls: The Essentials	\$5,162	\$7,226	\$11,184
Auditing Checkpoint Firewall - 1	\$5,162	\$7,226	\$11,184
Auditing Network Security: The Basics	\$5,162	\$7,226	\$11,184
Network Security Bootcamp for IT Auditors	\$22,367	\$31,314	\$48,463
Auditing Distributed and Web-Based Applications	\$14,139	\$19,794	\$30,634
Auditing SOLARIS	\$ 9,650	\$13,510	\$20,909
Auditing Windows and IIS	\$ 9,650	\$13,510	\$20,909
Auditing Windows	\$14,139	\$19,794	\$30,634
Auditing ORACLE Databases	\$ 9,650	\$13,510	\$20,909
IT Auditing with FISCAM & COBIT	\$11,894	\$16,652	\$25,771
Auditing Web Security	\$ 9,650	\$13,510	\$20,909
Freeware Hacking – (Hands-On)	\$15,635	\$21,888	\$33,876
Wireless Security	\$5,910	\$8,274	\$12,805
Intrusion Detection: From Start to Finish	\$5,910	\$8,274	\$12,805
Entity-Wide Security Program Planning & Management	\$8,150	\$11,415	\$17,667

PUBLIC SITE PRESENTATIONS (OPEN ENROLLMENT)	
SEMINAR TITLE	PRICE PER ATTENDEE
Introduction to IT Auditing	\$ 435
IT Audit Bootcamp	634
Auditing CISCO Routers	515
Auditing CISCO Routers: The Essentials	275
Auditing Firewalls	515
Auditing Firewalls: The Essentials	275
Auditing Checkpoint Firewall - 1	275
Auditing Network Security: The Basics	275
Network Security Bootcamp for IT Auditors	1,193
Auditing Distributed and Web-Based Applications	754
Auditing SOLARIS	515
Auditing Windows and IIS	515
Auditing Windows	754
Auditing ORACLE Databases	515
IT Auditing with FISCAM & CO	634
Auditing Web Security	515
Freeware Hacking – (Hands-On)	834
Wireless Security	315
Intrusion Detection: From Start to Finish	315
Entity-Wide Security Program Planning & Management	435

Terms and Conditions

Applicable to Information Technology

Professional Services (SIN 132-51)

1. SCOPE

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

2. PERFORMANCE INCENTIVES

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

3. ORDERING PROCEDURES FOR SERVICES (REQUIRING A STATEMENT OF WORK) (G-FCI-920) (MAR 2003)

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

When ordering services over \$100,000, Department of Defense (DOD) ordering offices and non-DOD agencies placing orders on behalf of the DOD must follow the policies and procedures in the Defense Federal Acquisition Regulation Supplement (DFARS) 208.404-70 – Additional ordering procedures for services. When DFARS 208.404-70 is applicable and there is a conflict between the ordering procedures contained in this clause and the additional ordering procedures for services in DFARS 208.404-70, the DFARS procedures take precedence.

GSA has determined that the prices for services contained in the contractor's price list applicable to this Schedule are fair and reasonable. However, the ordering activity using this contract is responsible for considering the level of effort and mix of labor proposed to perform a specific task

being ordered and for making a determination that the total firm-fixed price or ceiling price is fair and reasonable.

(a) When ordering services, ordering activities shall—

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

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

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

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

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

(2) Transmit the Request to Contractors:

Based upon an initial evaluation of catalogs and price lists, the ordering activity should identify the contractors that appear to offer the best value (considering the scope of services offered, pricing and other factors such as contractors' locations, as appropriate) and transmit the request as follows:

NOTE: When buying IT professional services under SIN 132—51 ONLY, the ordering office, at its discretion, may limit consideration to those schedule contractors that are small business concerns. This limitation is not applicable when buying supplies and/or services under other SINS as well as SIN 132-51. The

limitation may only be used when at least three (3) small businesses that appear to offer services that will meet the agency's needs are available, if the order is estimated to exceed the micro-purchase threshold.

(i) The request should be provided to at least three (3) contractors if the proposed order is estimated to exceed the micro-purchase threshold, but not exceed the maximum order threshold.

(ii) For proposed orders exceeding the maximum order threshold, the request should be provided to additional contractors that offer services that will meet the ordering activity's needs.

(iii) In addition, the request shall be provided to any contractor who specifically requests a copy of the request for the proposed order.

(iv) Ordering activities should strive to minimize the contractors' costs associated with responding to requests for quotes for specific orders. Requests should be tailored to the minimum level necessary for adequate evaluation and selection for order placement. Oral presentations should be considered, when possible.

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

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

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

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

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

(ii) MULTIPLE BPAs: When the ordering activity determines multiple BPAs are needed to meet its requirements, the ordering activity should determine which contractors can meet any technical qualifications before establishing the BPAs. When establishing the BPAs, the procedures in (a)(2) above must be followed. The procedures at (a)(2) do not apply to orders issued under multiple BPAs. Authorized users must transmit the request for quote for an order to all BPA holders and then place the order with the Schedule contractor that represents the best value.

- (2) Review BPAs Periodically: Such reviews shall be conducted at least annually. The purpose of the review is to determine whether the BPA still represents the best value. (See FAR 8.404)
- (c) The ordering activity should give preference to small business concerns when two or more contractors can provide the services at the same firm-fixed price or ceiling price.
- (d) When the ordering activity's requirement involves both products as well as executive, administrative and/or professional, services, the ordering activity should total the prices for the products and the firm-fixed price for the services and select the contractor that represents the best value. (See FAR 8.404)
- (e) The ordering activity, at a minimum, should document orders by identifying the contractor from which the services were purchased, the services purchased, and the amount paid. If other than a firm-fixed price order is placed, such documentation should include the basis for the determination to use a labor-hour or time-and-materials order. For ordering activity requirements in excess of the micro-purchase threshold, the order file should document the evaluation of Schedule contractors' quotes that formed the basis for the selection of the contractor that received the order and the rationale for any trade-offs made in making the selection.

4. ORDER

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

5. PERFORMANCE OF SERVICES

- a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering 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 of each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.
- d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

6. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

(a) The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

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

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

- (1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
- (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

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

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

7. INSPECTION OF SERVICES

The Inspection of Services–Fixed Price (AUG 1996) clause at FAR 52.246-4 applies to firm-fixed price orders placed under this contract. The Inspection–Time-and-Materials and Labor-Hour (JAN 1986) (Deviation – May 2003) clause at FAR 52.246-6 applies to time-and-materials and labor-hour orders placed under this contract.

8. RESPONSIBILITIES OF THE CONTRACTOR

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Deviation – May 2003) Rights in Data – General, may apply.

9. 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 Services.

10. INDEPENDENT CONTRACTOR

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

11. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

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

12. INVOICES

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

13. 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 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) 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 52.232-7 (DEC 2002), (Alternate II – Feb 2002) (Deviation – May 2003) applies to labor-hour orders placed under this contract.

14. RÉSUMÉS

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

15. INCIDENTAL SUPPORT COSTS

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

16. 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.

17. DESCRIPTION OF IT SERVICES AND PRICING

17.1 IT PROFESSIONAL SERVICES

SecureIT specializes in securing computer networks and the mission critical information they contain. We offer services and solutions focusing on the challenges associated with IT security, Cyber Security and IT governance. SecureIT designs enterprise security programs, implements best practices and performs security management for our customers. SecureIT has extensive experience in information security and IT audit of the financial services industry and financial management in the Federal Government. The SecureIT primary service offerings include:

Security Governance, Risk and Compliance Services and Solutions

- Security program management: Devise enterprise strategy which is integrated with enterprise architecture, and consistent with national and Department-level policy and standards.
- Security policy review, development and implementation: Update and maintain enterprise security policy to keep current with policy updates and threats. Provide implementation guidance and outreach to facilitate its effective implementation.
- Security framework implementation: Implement national standard and industry management frameworks such as NIST, ITIL, ISO and COBIT to improve control, increase visibility, and increase efficiency.
- Security requirements management: Analyze, adopt and manage all security and privacy requirements applicable to the enterprise. Provide support, tools and solutions to program officials and system implementers to efficiently “build security into” systems and applications.
- Risk management: Identify threats and weaknesses which could negatively impact enterprise missions, business processes and critical infrastructures. Implement risk management methods to ensure mission and business owners have the necessary information to make informed risk management decisions. Provide security reviews and assessments of contracted / outsourced services to identify risks to the agency.
- Regulatory compliance management: Provide expert services to assess organization compliance with applicable policies, requirements, and standards such as FISMA, FISCAM,

OMB circulars and memos, Privacy Act, HIPAA, SOX, and PCI-DSS. Implement technology solutions to permit efficient oversight, management and reporting over these initiatives.

- Acquisition planning and support for security: Provide security subject matter expertise through acquisition and procurement to effectively and cost-efficiently define security roles, requirements, desired outcomes and performance measures.
- Audit Liaison: Support the CIO and CISO as a liaison for all information security audits, assessments and reviews. Provide audit readiness services to proactively self-assess control adequacy. Decrease impact on program and operational personnel, improve communication, and eliminate process redundancies.

Information Assurance & Privacy Services and Solutions

- Organizational and common security control definition and implementation
- Categorization of information and systems to identify security impact level (FIPS PUB 199) or mission assurance category (DOD 8500)
- Security planning and development of effective system security plans (SSP) and System Security Authorization Agreements (SSAA)
- Interconnection analysis and development of agreements
- Risk assessment and management
- Contingency planning and testing
- Privacy Impact Assessments
- Security testing and evaluation (ST&E) per NIST SP 800-53A and DOD 8500
- Certification and Accreditation (C&A) in accordance with NIST, DIACAP, CNSS and agency-specific policy
- Security information, audit and event management
- System security support such as information systems security officer (ISSO) and information assurance security officer (IASO)

Enterprise Cyber Security Services and Solutions

- Asset Discovery: Identify, associate and manage your asset inventory.
- Data Discovery: Discover and classify/categorize data on networks and databases.
- Vulnerability Assessment and Management: Perform vulnerability assessment and management of networks, commercial and open source applications, databases, and custom software.
- Penetration Testing: Perform penetration testing to discover weaknesses and collaborate with your team to identify rapid and effective remediation.

- Security Configuration Management: Harden platforms through security configuration assessment. Identify changes and deviations which are then assessed for risk and appropriately documented.
- Database Security: Deploy and operate enterprise solutions for database security monitoring, control and auditing. Implement solutions to protect sensitive and classified data.
- Log Management: Provide solutions to automate and enhance security and event log management which comply with policies, regulations and mandates.
- Forensics and Incident Response: Assess damage and properly respond to security and privacy incidents and data breaches.

IT Audit Services

- IT audit strategy and planning: Develop strategic, annual and project-specific IT audit plans that integrate seamlessly with your organization's overall audit approach, and address executive and congressional priorities and concerns..
- Infrastructure and application audits: Our IT audit experts have the knowledge and expertise to audit nearly any network, operating system, application or security process. Enterprise infrastructure, internet applications, wireless networks, mission systems, and cloud computing outsourced services are a few examples of systems our team has audited. We follow government and industry recognized audit standards and practices, and oftentimes identify hybrid audit approaches to effectively audit emerging technology and outsourced services.
- FISMA: Through either outsourcing or co-sourcing arrangements, SecureIT performs IT audits for the Federal Information Security Management Act (FISMA). Our team can address all areas of FISMA spanning entity, component and system level reviews of Program, Policy, Standards, Inventory, C&A, Contingency, Incident Response, Plan of Action and Milestones, Training, and Security Configuration.
- OMB A-123 & Internal Control Assessments: Our team is well versed in OMB A-123, A-127 and A-130 policy and can assist your agency with its assessment of internal control activities. We understand commonly accepted control and control assessment frameworks such as FISCAM, and can ensure that IT controls are designed appropriately, operating effectively, and support compliance with applicable laws and regulations.
- Data mining and analysis: Our team employs Computer Assisted Audit Techniques (CAATs) to perform data analysis and data mining to identify trends and pinpoint anomalies. These services can be used to support audits or periodic monitoring of controls.

Training Services

SecureIT offers numerous custom training programs and seminars throughout the year. We provide superior, practical training on a broad variety of topics and technologies in order to help our clients

increase the information security, security assessment and IT audit skills of their staff. Our capabilities span:

- Security training program development, implementation and measurement
- Security course development
- Leveraged use of in-house and hosted e-learning
- Classroom instruction
- Technical security training
- Security and privacy awareness training

SecureIT's training solutions allow us to share our experience and understanding with our clients and professional communities in a range of locales and contexts. For maximum usefulness, our information-packed course offerings are assurance-focused and modular, and supported by high quality supplementary information and resources.

17.2 COMMERCIAL JOB TITLES (LABOR CATEGORIES)

SecureIT offers professionals in the following labor categories who can provide the skill sets needed to satisfy your professional services requirements.

Commercial Job Title: Project Manager – Level II

Minimum/General Experience: Minimum of eight years general experience, of which at least five years must be specialized in IT security field. Specialized experience includes: practical experience in managing security projects, project development, management and control of project funds and resources, demonstrated capability in managing multi-task projects of various complexity.

Functional Responsibility: Serves as the authorized interface with the customer agency's Contracting Officer's Representative and technical representatives. Responsible for ensuring work standards; assigns contractor staff tasking; resolves work discrepancies; supervises assigned contractor personnel; prepares required reports; and communicating policies, purpose and goals of the organization to subordinates. Applies corporate and customer quality assurance standards.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline. Associate's degree, or CISA or CISSP certification and four years additional relevant general experience in lieu of a BS/BA degree. Master's degree may be substituted for four years of general and three years of specialized experience.

Commercial Job Title: Project Manager – Level I

Minimum/General Experience: Minimum of six years general experience, of which at least four years must be specialized in IT security field. Specialized experience includes: practical experience in managing security projects, project development, management and control of project funds and resources, demonstrated capability in managing multi-task projects of various complexity.

Functional Responsibility: Serves as the authorized interface with the customer agency's Contracting Officer's Representative and technical representatives. Responsible for ensuring work standards; assigns contractor staff tasking; resolves work discrepancies; supervises assigned contractor personnel; prepares required reports; and communicating policies, purpose and goals of the organization to subordinates. Applies corporate and customer quality assurance standards.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline. Associate's degree, or CISA or CISSP certification and three years additional relevant general experience in lieu of a BS/BA degree. Master's degree may be substituted for three years of general and two years of specialized experience.

Commercial Job Title: **Principal Cybersecurity Consultant**

Minimum/General Experience: Minimum of fifteen (15) years of progressive experience supporting information technology projects with at least four (4) years related to information and computer security.

Functional Responsibility: Assists CIOs, CISOs and Program Managers to assess, develop, implement and maintain enterprise information / cyber security programs. Assist clients to interpret federal policies and standards related to information and cyber security. Develop strategies for implementing all aspects of Federal government cyber security programs (FISMA) as well as Privacy. Devise solutions to speed adoption of standards, policy and procedures as well as measure performance and compliance. Develop policy, procedures, and best practices. Prepare presentations, papers and other materials to support the CIO, CISO and program managers to communicate policy, requirements, practices and solutions to business and system owners. Program security program office support ranging from analysis, planning, and budget. Manage project requirements, resources and deliverables. Prepare and provide management and project reports.

Minimum Education: Master's degree in computer science, MIS, engineering, accounting information systems, or a related discipline.

Commercial Job Title: **Senior Cybersecurity Consultant**

Minimum/General Experience: Minimum of ten (10) years of progressive experience supporting information technology projects with at least four (4) years related to information and computer security.

Functional Responsibility: Assists CIOs, CISOs and Program Managers to assess, develop, implement and maintain enterprise information / cyber security programs. Assist clients to interpret federal policies and standards related to information and cyber security. Develop strategies for implementing all aspects of Federal government cyber security programs (FISMA) as well as Privacy. Perform application and network vulnerability testing to identify weaknesses. Devise solutions to protect networks, applications, information and business processes. Provide technical leadership and direction in support of project manager.

Minimum Education: Master's degree in computer science, MIS, engineering, accounting information systems, or a related discipline.

Commercial Job Title: Senior Cybersecurity Engineer

Minimum/General Experience: Minimum of eight (8) years of progressive experience supporting information technology projects with at least four (4) years experience related to information or computer security.

Functional Responsibility: Provides direct support for engineering, implementing, integrating and operating cyber security solutions for Federal government agencies. Responsibility may span network and system security engineering; design of technical solutions for network boundary protection, endpoint security, access control, auditing, log management, event management and correlation, and network monitoring; network and system vulnerability assessment; application and software security assessment ; database security assessment and monitoring; software security assurance; security configuration assessment, and compliance management; incident handling, response and reporting; technical security support to Certification and accreditation (C&A) processes and testing and security impact assessments as part of change management.

Minimum Education: Bachelor's degree in computer science, math, MIS, engineering, accounting information systems, or a related discipline.

Commercial Job Title: Cybersecurity Engineer

Minimum/General Experience: Minimum of three (3) years of experience supporting information technology projects in system design, engineering or operations with at least one (1) year of experience related to information or computer security.

Functional Responsibility: Provides direct support for engineering, implementing, integrating and operating cyber security solutions for Federal government agencies. Responsibility may span design of technical solutions for network boundary protection, endpoint security, access control, auditing, log management, event management and correlation, and network monitoring; network and system vulnerability assessment; application and software security assessment ; database security assessment and monitoring; software security assurance; security configuration assessment, and compliance management; incident handling, response and reporting; technical security support to Certification and accreditation (C&A) processes and testing and security impact assessments as part of change management.

Minimum Education: Bachelor's degree in computer science, math, MIS, engineering, accounting information systems, or a related discipline.

Commercial Job Title: Technical IT Auditor

Minimum/General Experience: Minimum of five years of IT systems, IT audit, or financial audit general experience and one year of specialized experience assisting audit teams in the use of computer assisted audit software, database design and management, and accounting software implementation.

Functional Responsibility: Participates in the performance of security risk assessments, system threat assessments, vulnerability assessments, and penetration analyses of facilities. Possesses a strong knowledge of information security fundamentals, platform security (UNIX, Windows NT/2K, web servers) and network security concepts and technologies. Analyzes technical security configuration information and identifies vulnerabilities and risks.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline.

Commercial Job Title: **Enterprise Consultant**

Minimum/General Experience: Eight years of IT systems or IT audit experience. Highly qualified at defining specialized requirements, conceptualizing and developing system designs, and analyzing complex computing environments. Knowledgeable in a wide range of hardware, software, and communications platforms.

Functional Responsibility: Has a good understanding of complex, multi-platform information technology processing environments. Deploys solutions and demonstrates ability to solve unanticipated complications in the field. Manages teams effectively, and ensures the integrity of delivered services. Highly competent in the area of IT audit and/or IT security.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline.

Commercial Job Title: **Senior IT Audit Consultant**

Minimum/General Experience: Five years of IT systems, IT audit, or financial audit experience.

Functional Responsibility: Includes independently performing a major segment of an audit, directing and instructing the work of senior and junior level auditors, and reviewing the work done to ensure it is of highest quality and delivered in a timely manner. The Senior IT Audit Consultant makes final decisions on all auditing and reporting matters.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline.

Commercial Job Title: **Staff IT Audit Consultant**

Minimum/General Experience: Three years of IT systems, IT audit, or financial audit experience.

Functional Responsibility: Includes independently performing a major segment of an audit, directing and instructing the work of junior level auditors, and reviewing the work done to ensure it is of highest quality and delivered in a timely manner. The Staff IT Audit Consultant makes decisions on routine auditing and reporting matters.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline.

Commercial Job Title: IT Security Consultant

Minimum/General Experience: Five years performing investigative analyses, evaluations, and audits, and associated remediation development, of computer systems in the areas of security, operations, hardware, application and system software design, development, and programming.

Functional Responsibility: Independently performs or leads a team in performing risk analysis and security audit services. Independently develops or supervises the development of security assessment reports. Analyzes security risks, defines security requirements, and designs, develops, and implements security solutions. Leads and participates in the performance of security risk assessments, system threat assessments, vulnerability assessments, and penetration analyses of facilities. Leads and participates in the use of security evaluation and assessment technology, techniques, and tools for the purposes of perform these duties.

Minimum Education: Bachelor's degree in computer science, accounting information systems, or a related discipline.

Commercial Job Title: Information Systems Security Officer (ISSO)

Minimum/General Experience: Minimum of five (5) years of progressive experience supporting information technology projects with a minimum of two (2) related to information and computer security.

Functional Responsibility: Performs security management and oversight on federal government computer systems. Responsibilities span certification and accreditation (C&A) of federal government systems which include: developing and updating security and contingency plans; performing privacy impact assessments, testing and assessment of security controls to support continuous monitoring; system and database audit review and monitoring; system security configuration assessment and monitoring; security impact assessment as part of system change management process; support for incident detection, handling and response; plan of action and milestone (POA&M) development and update to include corrective action planning; security training planning and reporting; and FISMA audit support.

Minimum Education: Bachelor's degree.

Commercial Job Title: Senior Information Assurance Analyst

Minimum/General Experience: Minimum of five (5) years of progressive experience supporting information technology projects with a minimum of two (2) related to information and computer security.

Functional Responsibility: Responsible for organizing, planning, implementing and maintaining the Cyber security program of Federal government agencies. Individuals support the Project Manager and/or Technical Lead in conducting a wide range of information security, information assurance and compliance activities that include: security program development, policy development and maintenance; review POA&Ms, incident reporting, and associated FISMA performance metrics for organization to identify issues and trends; system security planning and documentation; assist development and operations teams with security control implementation; security testing, control testing and assessment per NIST SP 800-53A or DOD 8500; Certification and accreditation (C&A) of agency systems per NIST SP 800-37 or DIACAP; security configuration assessment, management and reporting; security training program development, management and reporting; and prepare monthly, quarterly and annual FISMA and Privacy reporting.

Minimum Education: Bachelor's degree.

Commercial Job Title: Information Assurance Analyst

Minimum/General Experience: Minimum of two (2) years of experience supporting information technology projects in areas related to information assurance.

Functional Responsibility: Provides support to senior personnel and project managers for organizing, planning, implementing and maintaining the Cyber security program of Federal government agencies. Under direction of senior personnel, individuals perform information security, information assurance and compliance activities that include: security program development, policy development and maintenance; review POA&Ms, incident reporting, and associated FISMA performance metrics for organization to identify issues and trends; system security planning and documentation; assist development and operations teams with security control implementation; security testing, control testing and assessment per NIST SP 800-53A or DOD 8500; Certification and accreditation (C&A) of agency systems per NIST SP 800-37 or DIACAP; security configuration assessment, management and reporting; security training program development, management and reporting; and prepare monthly, quarterly and annual FISMA and Privacy reporting.

Minimum Education: Bachelor's degree.

Allowable Substitutions

The Table below presents the allowable substitutions based on the education and experience of the labor categories in this Pricelist. Experience should be professional and job related, however it does not have to be specific to the project to be accomplished. However, if a degree is used in place of experience, the degree must be related to the project or task.

Minimum Education Degree	Education and/or Experience	Related Certification
Associates	3 years relevant experience	Trade/Vocational School or Technical Training or Military Training in relevant field
Bachelors	Associates + 3 years relevant experience or 5 years relevant experience	Professional or Industry Standard Technical Certification in a relevant field. (e.g. CISSP, CISM, CISA, MCSE, CCNP, CNA, CNE)
Masters	Bachelors + 2 years relevant experience, or Associates + 5 years relevant experience, or 8 years relevant experience	Professional License (e.g. Certified Public Accountant, Professional Engineer)
Doctorate	Masters + 2 years relevant experience, or Bachelors + 5 years relevant experience, or Associates + 8 years relevant experience, or 10 years relevant experience	

Each professional or Industry standard technical certification in a relevant field (e.g. CISSP, CISA, CISM, MCSE, CCNP, CAN, CNE) is equivalent to one year of relevant experience.

17.3 PRICES FOR IT PROFESSIONAL SERVICES AT HOURLY RATES

The following hourly labor rates for each SecureIT labor category are applicable to customer-site (on-site) operations.

LABOR CATEGORIES	LABOR RATE
Project Manager – Level II	\$ 161.47
Project Manager – Level I	\$144.97
Principal Cybersecurity Consultant	\$210.00
Senior Cybersecurity Consultant	\$195.00
Senior Cybersecurity Engineer	\$170.00
Cybersecurity Engineer	\$88.00
Technical IT Auditor	\$139.19
Enterprise Consultant	\$144.24
Senior IT Audit Consultant	\$126.95
Staff IT Audit Consultant	\$98.09
IT Security Consultant	\$115.41
Information Systems Security Officer	\$121.00
Senior Information Assurance Analyst	\$103.00
Information Assurance Analyst	\$73.00

USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

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

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

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

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

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

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

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact **Jim Graham, Senior VP, Federal Programs, SecureIT Direct: (703) 230-0734, Main: (703) 464-7010, e-mail jgraham@secureit.com, or fax (703) 464-5990.**

BPA NUMBER _____

**(CUSTOMER NAME)
BLANKET PURCHASE AGREEMENT**

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

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

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

(2) Delivery:

DESTINATION	DELIVERY SCHEDULE/DATES
_____	_____
_____	_____

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

(4) This BPA does not obligate any funds.

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

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

OFFICE	POINT OF CONTACT
_____	_____
_____	_____

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

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

(a) Name of Contractor;

(b) Contract Number;

(c) BPA Number;

(d) Model Number or National Stock Number (NSN);

(e) Purchase Order Number;

(f) Date of Purchase;

(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and

(h) Date of Shipment.

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

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

BASIC GUIDELINES FOR USING “CONTRACTOR TEAM ARRANGEMENTS”

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

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

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

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

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

Here is a general outline on how it works:

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