ACE
Academy of Computer Education

AUTHORIZED FEDERAL SUPPLY SERVICE
INFORMATION TECHNOLOGY SCHEDULE PRICELIST
GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY
EQUIPMENT, SOFTWARE AND SERVICES

SIN 132-50 - TRAINING COURSES FOR INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE (FPDS Code U012)

SHD Holdings, LLC
T/A
ACADEMY OF COMPUTER EDUCATION
7833 WALKER DR STE 520-C
GREENBELT, MD 20770
CAGE Code: 44P59 • DUNS: 04-018-8315
Phone: 301-220-2801
Fax: 301-220-3814
E-mail: rsita@trainace.com
Web: www.trainace.com

Contract Number: GS-35F-0431S

Period Covered by Contract: May 24, 2006 to May 23, 2021

General Services Administration
Federal Supply Service

Pricelist current through Refresh/Modification #40, dated 09/16/16.

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

TABLE OF CONTENTS

INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM 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.fss.gsa.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Supply Service Home Page (www.fss.gsa.gov) contain information on a broad array of products and services offered by small business concerns.

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

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

1.   Geographic Scope of Contract:

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

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

Offerors are requested to check one of the following boxes:
> [ ]   The Geographic Scope of Contract will be domestic and overseas delivery.
> [ ]   The Geographic Scope of Contract will be overseas delivery only.
> [X]   The Geographic Scope of Contract will be domestic delivery only.

2.   Contractor's Ordering Address and Payment Information:

ACADEMY OF COMPUTER EDUCATION
7833 WALKER DR STE 520-C
GREENBELT, MD 20770

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

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

301-220-2802

3.   LIABILITY FOR INJURY OR DAMAGE

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

4.   Statistical Data for Government Ordering Office Completion of Standard Form 279:

Block 9: G. Order/Modification Under Federal Schedule
Block 16: Data Universal Numbering System (DUNS) Number: 04-018-8315
Block 30: Type of Contractor - B

A.	Small Disadvantaged Business
B.	Other Small Business
C.	Large Business
G.	Other Nonprofit Organization
L.	Foreign Contractor

Block 31: Woman-Owned Small Business - No
Block 36: Contractor's Taxpayer Identification Number (TIN): 52-2331811

4a.   CAGE Code: 44P59
4b.   Contractor has registered with the Central Contractor Registration Database.

5.   FOB Destination

6.   DELIVERY SCHEDULE

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

SPECIAL ITEM NUMBER	DELIVERY TIME (Days ARO)
132-50	As negotiated with ordering activity

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

7.   Discounts: Prices shown are NET Prices; Basic Discounts have been deducted.

a.	Prompt Payment: ½% - 15 days from receipt of invoice or date of acceptance, whichever is later.
b.	Quantity: None
c.	Dollar Volume: None
d.	Government Educational Institutions: None
e.	Other

8.   Trade Agreements Act of 1979, as amended:

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

9.   Statement Concerning Availability of Export Packing:

10.   Small Requirements: The minimum dollar value of orders to be issued is $1,092.00.

11.   Maximum Order (All dollar amounts are exclusive of any discount for prompt payment.)

The Maximum Order value for the following Special Item Numbers (SINs) is $25,000:

Special Item Number 132-50 - Training Courses

12.   ORDERING PROCEEDURES FOR FEDERAL SUPPLY SCHEDULE CONTRACTS

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

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

b.   FAR 8.405-2 Ordering procedures for services requiring a statement of work.

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

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

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

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

(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.

5

(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.

   NOTE: Refer to FAR Part 31.205-46 Travel Costs, for allowable costs that pertain to official company business travel in regards to this contract.

(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 52.212-4, paragraphs (l) Termination for the ordering activity's convenience, and (m) Termination for Cause (See C.1.)

16.   GSA Advantage!

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

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

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

17.   PURCHASE OF OPEN MARKET ITEMS

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

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

> (1)   All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));

> (2)   The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;

> (3)   The items are clearly labeled on the order as items not on the Federal Supply Schedule; and

> (4)   All clauses applicable to items not on the Federal Supply Schedule are included in the order.

18.   CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS

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

> (1)   Time of delivery/installation quotations for individual orders;

> (2)   Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/ service/software package submitted in response to requirements which result in orders under this schedule contract.

> (3)   Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

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

19.   OVERSEAS ACTIVITIES

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

_____

_____

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

20.   BLANKET PURCHASE AGREEMENTS (BPAs)

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

21.   CONTRACTOR TEAM ARRANGEMENTS

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

22.   INSTALLATION, DEINSTALLATION, REINSTALLATION

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

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

23.   SECTION 508 COMPLIANCE.

If applicable, Section 508 compliance information on the supplies and services in this contract are available in Electronic and Information Technology (EIT) at the following:

ACE is building its Section 508 compliance at this time.

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

24.   PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES.

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

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

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

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

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

(1) For such period as the laws of the State in which this contract is to be performed prescribe; or

(2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

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

26. SOFTWARE INTEROPERABILITY.

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

27. ADVANCE PAYMENTS

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

TERMS AND CONDITIONS APPLICABLE TO PURCHASE OF TRAINING COURSES FOR GENERAL PURPOSE COMMERCIAL INFORMATION TECHNOLOGY EQUIPMENT AND SOFTWARE (SPECIAL ITEM NUMBER 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.   **If applicable** For hands-on training courses, there must be a one-to-one assignment of IT equipment to students.

c.   The Contractor shall provide each student with a Certificate of Training at the completion of each training course.

d.   The Contractor shall provide the following information for each training course offered:

(1)   The course title and a brief description of the course content, to include the course format (e.g., lecture, discussion, hands-on training);

(2)   The length of the course;

(3)   Mandatory and desirable prerequisites for student enrollment;

(4)   The minimum and maximum number of students per class;

(5)   The locations where the course is offered;

(6)   Class schedules; and

(7)   Price (per student, per class (if applicable)).

e.   For those courses conducted at the ordering activity's location, instructor travel charges (if applicable), including mileage and daily living expenses (e.g., per diem charges) are governed by Pub. L. 99-234 and FAR Part 31.205-46, and are reimbursable by the ordering activity on orders placed under the Multiple Award Schedule, as applicable, in effect on the date(s) the travel is performed. Contractors cannot use GSA city pair contracts. The Industrial Funding Fee does NOT apply to travel and per diem charges.

9.   "NO CHARGE" TRAINING

The Contractor shall describe any training provided with equipment and/or software provided under this contract, free of charge, in the space provided below. **None**

COURSE DESCRIPTIONS

A+ and Network+ Courses

The A+/ Network+ program provides the student with a solid foundation in PC hardware and operating system knowledge (DOS / Windows 9x, 2000, NT 4.0 and XP), as well as the hands-on training necessary to succeed in the IT industry. Additional program hours in networking concepts, combined with application software, makes the A+/ Network+ certification program an excellent stepping stone to more advanced certifications. To receive the A+ certification students must pass two tests — Core Hardware and Operating Systems.

Network+ is a certification that ensures the knowledge of networking professionals with 18—24 months' experience in the IT industry, or those that possess equivalent knowledge and skills. Network+ is an entry level certification open to anyone who desires to learn networking basics as a foundation which can be applied towards other advanced certifications.

A+ and Network+ certification provides IT managers and supervisors with an increasingly important benchmark in the hiring and promotion process. What's more, companies are finding that incorporating certified technicians within their organizations helps build confidence and value. More and more companies are requiring computer certifications, such as A+, Network+ as a pre-requisite for employment. The last two hours of the Courses will be spent doing test prep and review.

Security+

This vendor neutral training course is designed for network and security administrators and those with similar job functions who have experience with general networking and basic security knowledge. This CompTIA Security+ course will educate the student on critical security concepts and is mapped to the exam to teach the student the language, theory and principles of the following domains:

- General security concepts
- Communications security
- Infrastructure security
- Basics of cryptography
- Operational and organizational security

With the new computer privacy laws all industries and agencies can benefit by employing a security specialist. In today's environment it has become an absolute must to implement and maintain security technologies and policies. Security+ takes the first step in teaching you to implement and monitor security on networks and computer systems, and respond to security breaches in the appropriate manner.

Linux+

The CompTIA Linux+ certification is a new standard of competency for technicians with six-months experience installing, operating and maintaining Linux operating systems. ACE's Linux+ training course will help you meet the certification requirements and prepare you for the exam.

The Linux+ certification validates technical competency and provides a broad awareness of Linux operating systems. Those holding Linux+ certification demonstrate critical knowledge of installation, operation, administration and troubleshooting services.

The demand for Linux support professionals will continue to grow as companies integrate Linux as a low cost alternative for both the client and server side of their networks.

This program presents you with the concepts and skills necessary to install and configure a Linux operating system. Not only is Linux becoming a low cost alternative for client machines but also it is rapidly taking a hold of the Internet as a stable web server.

Microsoft Certified Solutions Associate (MCSA)

The (MCSA) credential is the premier certification for professionals who successfully implement, manage, and troubleshoot the ongoing needs of Microsoft client and server-based operating environments. Implementation responsibilities include installing, configuring, and troubleshooting network systems. The MCSA course program is designed to prepare students for positions in network administration and network management.

Cisco Certified Network Administrator (CCNA)

The CCNA certification (Cisco Certified Network Associate) indicates a foundation in and apprentice knowledge of networking. CCNA certified professionals can install, configure, and operate LAN, WAN, and dial access services for small networks (100 nodes or fewer), including but not limited to use of these protocols: IP, IGRP, Serial, Frame Relay, IP RIP, VLANs, RIP, Ethernet, Access Lists. The last two hours of the Courses will be spent doing test prep and review.

Cisco Certified Network Professional (CCNP)

In the WAN service and support arena, Cisco certification assures proficiency in supporting Internetworks. Becoming a Cisco professional tells the customer or employer that you have passed Cisco's strict testing requirements. The CCNP title is for the network professional looking to stand out from the crowd and demonstrate their mastery of LAN and WAN technologies.

Cisco requires many vendors, re-sellers and support providers to have CCNP's on their staff because CCNP's are recognized throughout the industry as competent support professionals. Network customers can feel confident that the support the Cisco professional provides is tested, Cisco-certified knowledge

Cisco Certified Design Administrator (CCDA)

The Cisco Certified Design Associate (CCDA) course focuses on the skills needed to design world-class networks for small- to medium-sized networks. CCDA students will learn how to analyze an existing Internetwork and determine present and future customer needs.

Students will design network solutions that include network topologies, LAN and WAN hardware and media, network-layer addressing, routing protocols, and network management strategies. The Designing Cisco Networks course is intended to prepare an individual to become a Cisco Certified Design Associate (CCDA).

Microsoft Office Specialist (MOS)

Microsoft Office Specialist certification (MOS, formerly referred to as MOUS) is the universally accepted standard assessment of desktop proficiency for the Microsoft office suite of applications. Office Specialist certification gives both job applicants and employees the advantage of proven productivity in a competitive market for jobs and advancement. When potential employees are certified, hiring managers know they can hit the ground running. They know time and money won't be wasted on training and support.

By encouraging individuals to develop advanced skills with Microsoft business desktop software, the Office Specialist program is helping to fill the demand for qualified, knowledgeable people in the workplace. Office Specialist also helps satisfy an organization's need for a qualitative assessment of employee skills.

Microsoft Office Specialist Expert (MOS Expert)

Microsoft Office Specialist (MOS/MOUS) Expert certification is the universally accepted standard assessment of desktop proficiency. Earning Office Specialist certification acknowledges you have the expertise to work with Microsoft Office programs. Office Specialist-certified individuals report increased competence and productivity with Microsoft Office programs as well as increased credibility with their employers, co-workers, and clients.

Office Specialist certification sets you apart in today's competitive job market, bringing employment opportunities, greater earning potential and career advancement, in addition to increased job satisfaction. Candidates must pass the Microsoft Expert exam in Word, Excel, or both to hold the title of MOS Expert in that application.

Project Management Professional (PMP)

The Project Management Professional Course prepares the student and satisfies the educational requirement for attaining the PMP® Certification through PMI; (PMP certification conducted by PMI (Project Management Institute) - the leading professional association in project management established in 1969, is the world's most recognized and respected professional credential for individuals associated with project management. In 1999, PMI became the first organization in the world to have its Certification Program attain International Organization for Standardization (ISO) 9001 recognition.

Microsoft Project (MS Project 2003)

This course will enable you to create and manage your projects in a standalone desktop environment. But to analyze projects, optimize resources, and prioritize work in a way that meets an organization's overall business objectives, you need to use a more encompassing project management solution. In this course, you will use

Microsoft Project Professional 2003 to create, coordinate, and communicate project information in a consistent and efficient manner within the framework of an Enterprise Project Management (EPM) environment.

Certified Wireless Network Administrator (CWNA)

CWNA is the foundation level wireless LAN certification for the industry standard CWNP Program. It is your starting point for wireless training and certification. CWNA covers a broad range of wireless LAN topics focused on 802.11 wireless technology rather than products of specific vendors. The Wireless LAN Administration course provides the networking professional a complete foundation of knowledge for entering into or advancing in the wireless networking industry.

Certified Ethical Hacker (CEH)

The CEH course explores the tactics commonly used to penetrate a network. The courseware maps to EC-Council's certification exam 312-50, and includes the official EC-Council Certified Ethical Textbook Volumes 1 & 2, an accompanying Lab Manual, a Linux OS CD, and 2 CD's containing over 300 of the latest hacking tools and exploits. This certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. CEH candidates will be immersed into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. Candidates will begin by understanding how perimeter defenses work and then be lead into scanning and attacking their own networks. No real network is harmed. Candidates then learn how intruders escalate privileges and what steps can be taken to secure a system. Candidates will also learn about Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation.

Certified Hacking Forensic Investigator (CHFI)

The CHFI course will help students understand the process of detecting hacking attacks, of properly extracting evidence to report the crime and of conducting audits to prevent future attacks. Computer Hacking Forensic Investigator enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud. The CHFI course will provide participants the necessary skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.

Certified Information System Security Professional (CISSP)

CISSP is the term used for the (Certified Information System Security Professional). The International Information Systems Security Certification Consortium, Inc., or (ISC)², is a non-profit organization, incorporated in the Commonwealth of Massachusetts, based in Palm Harbor, Florida. (ISC)² is dedicated to:

- Maintaining the CBK$^®$ for information security,
- Certifying industry professionals and practitioners under an international standard,
- Providing education,
- Administering certification examinations, and
- Ensuring the continued competence of credential holders.

Governments, corporations, centers of higher learning and organizations worldwide demand staff that have a common knowledge platform for and demonstrate competence of the dynamic nature of information security.

(ISC)² helps fulfill these requirements. (ISC)^2 promotes the CISSP exam as an aid to evaluating personnel performing information security functions.

Live-Online Cyber War

The Cyber War, advanced penetration testing training class is an intense, hands -on training class that makes traditional pentesting training classes look like a Security+ class. The class was written by a conglomerate of IT security and security training's most respected professionals. This team of industry professionals were looking to create a course that dissects the art of hacking and creates professionals who deeply understand the "why's" of penetration testing / exploitation so that all traditional barriers can be broken.

Advanced Penetration testing 3 day

Advanced Penetration Testing Training, or APT training, is an intense, hands-on training class that makes traditional pentesting training classes look like a Security+ class. A three-day intensive course, our class teaches students how to attack and defend high-secured environments using advanced persistent threat

techniques that you never thought of. With an 80 percent hands-on delivery style, you'll gain the real-world experience you need to become a great pentester.

DIARMF Department of Defense Information Assurance Risk Management Framework

Department of Defense Risk Management Framework enables practitioners to immediately apply the training to their daily work. Each activity in the Risk Management Framework is covered in detail, as is each component of the documentation package and the continuous monitoring process. DoDI 8510.01, NIST 800-53 Security Controls and NIST 800-53a Evaluation Procedures are also covered in detail. Class participation exercises reinforce key concepts. RMF is designed for those who need to become proficient in the nuts and bolts of FISMA RMF implementation. This course provides the practical knowledge you need, without being slanted in favor of a specific software tool set.

Exploit Development

Exploit Development is a course that takes participants from minimal exposure to advanced concepts. The course will begin with simple, familiar concepts and expand rapidly into new more advanced areas. Students do not need vast programming experience to participate in Exploit Development training. Templates will be provided for each exploit with the intent being to cut down on raw programming time in class, and instead focusing more on the methodology and mindset that goes into writing the different exploits.

For students with a limited programming background and experience, worry not! Templates are provided for each exploit with the intent being to cut down on the raw programming time in class, and instead focusing more on the methodology and mindset that goes into writing these different exploits. By taking this approach, students can expect to learn and to execute 12-15 exploits over the duration of the class.

It is highly recommended that students have approximately two years of hacking or cyber security experience. This course is appropriate for Advanced IT Security Professionals (deep technical), IT Security Assessors (Penetration Testers), Application Developers, and Intrusion Analysts.

Honeynetting

You will see how the AV companies collect malware and its variants and get an introduction as to how they analyze it. The class will demonstrate a ZeuS (and SpyBot if time permits) attack from beginning to end with respect to the compromise. You will learn:

• What honeypots are
• What they are for
• The different types (You will get an overview but the class will focus on the research variants)
• How to target a particular bot and what is required to do so
• How hackers detect them and common things they do once the honeypot is detected
• How to process the data collected
• How to share the data collected

You will also be exposed to a lot more vectors that affect each of these areas. Finally, you will hear about some industry trends and what the current state of security is and where it is going.

Malware Analysis/Reverse Engineering

The goal of the AMA training class is to provide a methodical hands-on approach to reverse-engineering by covering both behavioral and code analysis aspects of the analytical process.

The course begins by looking into PE headers and how to handle DLL interactions. Then it moves on to the fundamentals of x86 architecture assembly. Next you learn to examine malicious code in order to understand the program's key components and execution flow. You then learn to identify common malware characteristics by looking at Windows API use patterns, and will examine excerpts from bots, rootkits, key loggers, and downloaders. From there you move on to standard and custom packers and other tools and techniques for bypassing anti-virus, and then on to malware with anti-debugging/anti-analysis capabilities. Then the class is concluded with obfuscated browser scripts.

Mobile Hacking

With our Mobile Hacking & Security training course, you'll learn how to bypass others' mobile security while learning how strength your own. This class covers hacking and security concepts on today's most popular cellular phone and mobile platforms, such as Android and iPhone. You'll learn the background behind the Android and iPhone environments, figure out how to exploit applications and attack web services via iDevices such as the iPod and iPad.

At the end of the course, you'll maintain a firm understanding of the security behind mobile devices and what you can do to exploit or protect it.

Python for Security Pros

Python has become such an integral development language in today's IT security landscape, a basic understanding of the language is a must-have for anyone looking to move into to the upper realms of penetration testing and IT security. You cannot be an advanced penetration tester without a firm

understanding of Python—it is vital to protecting your network. A firm grasp of Python enables the penetration tester to develop their own security—without having to rely on the limitations of someone else's. Individuals who are fluent in the Python language belong to an exclusive group of security professionals who are verified to protect a network at its fullest capability.

Our Python for Security Professionals training class will prepare the attendee with the skill set necessary to be dangerous in the security environment. Students will learn how to detect malware, discover vulnerabilities, and develop prototype code to attack or defend against a problem. Whether you have experience in programming or not, this course will meet you at your current skill level to ensure that you are able to customize and create open source tools as a certified, skilled and experienced penetration tester.

Secure Coding

This course lays the basic foundation required by all application developers and development organizations to produce applications with greater stability and posing lesser security risks to the consumer. The Certified Secure Application Developer standardizes the knowledge base for application development by incorporating the best practices followed by experienced experts in the various domains.

The distinguishing aspect of software security course is that unlike vendor or domain specific certifications, it exposes the aspirant to various programming languages from a security perspective. This drives greater appreciation for the platform / architecture / language one specializes on as well as an overview on related ones

Social Engineering and Social Manipulation

Noted as one of the fastest growing security threats, social engineering is dangerous because it relies on the manipulation of people—and not computers. Our course is designed to train individuals to reduce the number of those affected and to ensure the safety of your network. An intense, three-day hands on course, our Social Engineering & Manipulation training allows students to take on the role of a malicious hacker and perform various social engineering attacks to leverage sensitive information. Like real-world social engineering, you'll do things like research targets through social media, stage fake calls to gather information and set up fake websites that pertain to your target's interests. After successful completion of the course, students will be able to effectively identify, isolate and prevent social engineering threats from engaging their networks.

Threat Intelligence

With Advanced Security's Advanced Threat Intelligence Training, you won't have to second-guess your ability to go against the bad guys—your knowledge of threat intel will lead you to answers others wouldn't be able to deduce. Students in our program earn their expertise with an intense, three-day, hands-on, 8 hr/day program that educates on topics from the attack philosophy, principles of forecasting, host-based detections and reporting.

You'll learn the key processes and setups to ensure you can start collecting intelligence data in your own network right away, in a uniformed and actionable manner. This course is 70 percent hands-on and includes both group and individual labs. So when it's time to build your own threat intel network, you will know exactly how to execute the best strategy.

Wireless Security

Our Wireless Hacking and Security training course is a leading wireless security training class in the industry and was written under the guidance of extremely respected industry professionals. This class is continually updated to include some of the latest in wireless attacks and security principles. This is a three-day class and is primarily a hands-on, experiential class. Students will be taken through many different wireless attack techniques and security implementations and at the end of the class, will have a firm understanding of the most cutting edge wireless security principles.

Web application security

For people who are looking to expand their skill set a bit further beyond the Certified Ethical Hacker level, this class will teach you to apply manual processes to web applications that are commonly available for the purpose of penetration testing and intrusion. In our very hands-on focused web application security training class we will walk the students through the process of managing risks in web applications. We will show you how to identify and classify weaknesses in web apps. We also dive into strategies for secure web application development. Students should have a working knowledge of server and client networking, general network security principles as well as the software development life cycle.

SharePoint

This course will provide you with the knowledge and skills to configure and manage a Microsoft® SharePoint Server environment. This course will teach you how to configure SharePoint Server, as well as provide guidelines, best practices, and considerations that will help you optimize your SharePoint server deployment.

Business Continuity and Disaster Recovery

This course is about bout identifying vulnerabilities and managing failure risks. It covers topics such as

planning, designing, testing and, when necessary, implementing responses to interruptions of access or service and responses to disasters. Topics covered include preparation of a disaster recovery plan, assessing risks, making a plan and knowing and utilizing the different groups and individuals who implement such plans.

Computer Forensics Evidence Collection

A digital crime scene is quite different than that of a physical one, therefore specific expertise is necessary to maneuver within its environment. With our self-paced online Computer Forensics Analyst training, you'll learn tips for controlling a digital forensic investigation and techniques for seizing, collecting and protecting evidence. Working within a virtual environment, you'll use a wide range of forensic tools such as WinAudit, Helix, IEHistoryView, Paraben P2 Commander and Favorites View to identify and examine potential evidence like a real life digital crime scene. At the end of your course study, you'll be equipped with the skills to solve digital crimes as a Computer Forensics Analyst.

In order to be successful in this online training class, it is recommended that individuals have at least intermediate knowledge of the Windows & Linux operating systems and how computer hardware functions.

Ethical Hacking Tools and Techniques

Ethical Hacking Methods training course, you'll learn the methods, tools and techniques necessary to become a skilled ethical hacker trained to locate weaknesses in the most stringent of network environments. You'll cover topics ranging from the fundamentals of hacking, vulnerability scanning and exploits and network traffic analysis, to name a few. With full access to a live virtual lab environment, case studies, lectures and additional course content that mirrors real-life hacking scenarios, you'll become equipped with abundant knowledge to defend the networks, systems and applications of major organizations.

In order to be successful in this online training class, it is recommended that individuals possess general knowledge of server/client networking, firewalls and/or common types of malware.

Information Security and Risk Management

Running a business without a risk management plan is like running a marathon without drinking any water—it's designed to fail. IT professionals and business managers should be well-versed in risk management planning to ensure that their businesses do not fall victim to threats and vulnerabilities. With our Cyber Security Risk Management training, we teach the principles and methodology for creating an effective risk management plan in order to successfully balance business management and security.

You'll cover how to align risks, threats and vulnerabilities to one of the seven domains of a typical IT infrastructure and prioritize them based on their risk impact to an organization. Additionally, you'll learn about the COBIT P09 risk management objectives and use them to define the scope of risk management for a typical IT infrastructure. This will culminate in developing an IT risk management plan. At the completion of this course, you'll be fully prepared to make the best decisions for your business regarding risk management.

Locking Down Linux User Accounts, Filesystems, and Services

In this training course, we'll teach you how students will get hands-on training that will teach them how to configure and manage security on Linux systems. Students will cover everything from basic security controls, user management and security and Linux filesystem and services. At the end of the course, students will possess a solid understanding of the Red Hat Enterprise, Ubuntu, Fedora and CentOs, earning them a certificate of completion in Linux security.

In order to be successful in this online training class, it is recommended that individuals have at least 6 to 12 months of experience supporting Linux servers and clients.

Network Security Essentials

All the basics of network security are rolled up into this condensed, exciting class that will prepare you for the world of cyber security. Cover topics such as TCP/IP network protocols, threats, vulnerable access points, securing applications and the top tools to help harden a network.

Protecting Networks with Firewalls and VPNs

This class covers the ins and outs of the two most key technologies that protect networks these days, Virtual Private Networks (VPN) and Firewalls. Learn rules, fundamentals, filters, design and deployment strategies and secure remote access.

Protecting Windows Systems with Access Controls, Encryption, and Group Policy

The majority of businesses use Windows systems to host their networks. Malware authors know this and constantly attempt to exploit Windows systems at all times. This means there's a tremendous amount of responsibility for security professionals to employ the highest skill set possible in order to ensure safeguarding of highly sensitive data. Because Windows systems are constantly changing, it is important for security professionals to maintain a firm grasp on the security principles that guide Windows systems.

Topics range from authentication, encryption, access controls, application rules, and Group Policy objects.

PRODUCTS AND SERVICES PRICELIST
On-Site GSA discount rate table. Includes IFF. All rates are fully burdened.

FPDS	Course Name	Course Length	Base Year	Year 2	Year 3	Year 4	Year 5
U012	A+	56 hours	$ 1,315.00	$ 1,345.00	$1,375.00	$ 1,406.00	$ 1,438.00
U012	Network+	40 hours	$ 1,225.00	$ 1,253.00	$1,281.00	$ 1,310.00	$ 1,340.00
U012	A+ Network+ Combo	96 hours	$ 2,263.00	$ 2,314.00	$2,366.00	$ 2,420.00	$ 2,475.00
U012	Security+	40 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Linux+	40 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	CompTIA Advanced Security Practitioner	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Microsoft Certified Solutions Associate	96 hours	$ 4,167.00	$ 4,261.00	$4,357.00	$ 4,456.00	$ 4,557.00
U012	Cisco Certified Network Administrator (CCNA)	40 hours	$ 2,172.00	$ 2,221.00	$2,271.00	$ 2,322.00	$ 2,375.00
U012	Cisco Certified Network Professional (CCNP)	120 hours	$ 4,892.00	$ 5,003.00	$5,116.00	$ 5,232.00	$ 5,350.00
U012	Cisco Certified Design Administrator (CCDA)	40 hours	$ 1,628.00	$ 1,665.00	$1,703.00	$ 1,742.00	$ 1,781.00
U012	Microsoft Office Specialist (MOS)	40 hours	$ 1,537.00	$ 1,572.00	$1,608.00	$ 1,644.00	$ 1,681.00
U012	Microsoft Office Specialist Expert (MOS Expert)	32 hours	$ 1,719.00	$ 1,758.00	$1,798.00	$ 1,839.00	$ 1,881.00
U012	Project Management Professional (PMP)	40 hours	$ 2,263.00	$ 2,314.00	$2,366.00	$ 2,420.00	$ 2,475.00
U012	Microsoft Project (MSProj)	40 hours	$ 721.00	$ 737.00	$ 754.00	$ 771.00	$ 788.00
U012	Certified Wireless Network Administrator (CWNA)	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Certified Ethical Hacker (CEH)	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Computer Hacking Forensic Investigator (CHFI)	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Certified Information System Security Professional (CISSP)	40 hours	$ 2,263.00	$ 2,314.00	$2,366.00	$ 2,420.00	$ 2,475.00
U012	Live Online - Cyber War	32 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Live Online - Computer Hacking Forensic Investigator (CHFI)	40 hours	$ 1,175.00	$ 1,202.00	$1,229.00	$ 1,257.00	$ 1,285.00

PRODUCTS AND SERVICES PRICELIST
On-Site GSA discount rate table. Includes IFF. All rates are fully burdened.

FPDS	Course Name	Course Length	Base Year	Year 2	Year 3	Year 4	Year 5
1991	Live Online - Certified Ethical Hacker	40 hours	$ 1,991.00	$ 2,036.00	$2,082.00	$ 2,129.00	$ 2,177.00
U012	Live Online -Project Management Professional (PMP)	40 hours	$ 1,175.00	$ 1,202.00	$1,229.00	$ 1,257.00	$ 1,285.00
U012	Live Online -CompTIA Advanced Security Practitioner	40 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Live Online – Cisco Certified Network	40 hours	$ 1,537.00	$ 1,572.00	$1,608.00	$ 1,644.00	$ 1,681.00
U012	Live Online - Security+	40 hours	$ 1,356.00	$ 1,387.00	$1,418.00	$ 1,450.00	$ 1,483.00
U012	Live Online -Certified Information System Security Professional (CISSP)	40 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Advanced Penetration testing 3 day	24 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	DIARMF Department of Defense Information Assurance Risk Management Framework	40 hours	$ 2,268.00	$ 2,319.00	$2,371.00	$ 2,425.00	$ 2,480.00
U012	Exploit Development	40 hours	$ 3,628.00	$ 3,710.00	$3,794.00	$ 3,880.00	$ 3,968.00
U012	Honeynetting	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Malware Analysis/Reverse Engineering	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Mobile Hacking	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Python for Security pros	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Secure Coding	40 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Social Engineering and Social Manipulation 3 day	24 hours	$ 2,716.00	$ 2,777.00	$2,840.00	$ 2,904.00	$ 2,970.00
U012	Threat Intelligence 3 days	24 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Wireless Security	40 hours	$ 1,610.00	$ 1,646.00	$1,683.00	$ 1,721.00	$ 1,760.00
U012	Web Application Security Training 3 days	24 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Training room rental per day	24 hours	$ 590.00	$ 603.00	$ 617.00	$ 631.00	$ 645.00

PRODUCTS AND SERVICES PRICELIST
On-Site GSA discount rate table. Includes IFF. All rates are fully burdened.

FPDS	Course Name	Course Length	Base Year	Year 2	Year 3	Year 4	Year 5
U012	Training room rental per week	40 hours	$ 2,268.00	$ 2,319.00	$2,371.00	$ 2,425.00	$ 2,480.00
U012	SharePoint Training	32 hours	$ 1,809.00	$ 1,850.00	$1,892.00	$ 1,935.00	$ 1,979.00
U012	Business Continuity and Disaster Recovery Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Computer Forensics Evidence Collection Self-Paced and /or	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Ethical Hacking Tools and Techniques Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Information Security and Risk Management Planning Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Locking Down Linux User Accounts, Filesystems, and Services Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Managing Information Security Risks, Threats, and Vulnerabilities Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Network Security Essentials Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Protecting Networks with Firewalls and VPNs Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Protecting Windows Systems with Access Controls, Encryption, and Group Policy Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00
U012	Securing Web Applications Self-Paced and /or Classroom	30 hours	$ 907.00	$ 928.00	$ 949.00	$ 970.00	$ 992.00

USA COMMITMENT TO PROMOTE
SMALL BUSINESS
PARTICIPATION PROCUREMENT

PREAMBLE

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

COMMITMENT

To actively seek and partner with small businesses.

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

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

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small 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 **Ralph P. Sita Jr., Voice: (301) 220-2802, rsita@trainace.com, FAX: (301) 220-3814.**

<p style="text-align: center;">BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE</p>

(Insert Customer Name)

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

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

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

Signatures

_____		_____	
Ordering Activity	Date	Contractor	Date

(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 SCHEDULES / DATES

_____   _____
_____   _____
_____   _____

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

(4)   This BPA does not obligate any funds.

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

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

OFFICE   POINT OF CONTACT

_____   _____
_____   _____
_____   _____

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

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

        (a)   Name of Contractor;

        (b)   Contract Number;

        (c)   BPA Number;

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

        (e)   Purchase Order Number;

        (f)   Date of Purchase;

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

(h)   Date of Shipment.

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

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

****

BASIC GUIDELINES FOR USING
"CONTRACTOR TEAM ARRANGEMENTS"

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

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

Orders under a Team Arrangement are subject to terms and conditions 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 Schedules "Team Solution" to meet the customer's requirement.

- Customers make a best value selection.