Federal Supply Service
Information Technology Schedule 70

Authorized FSS Schedule Price List

Contract Number: GS-35F-0632T

Unatek, Inc.
1100 Mercantile Lane, Suite 115-A
Largo, MD 20774
www.unatek.com

Telephone: (301) 583-4629
Fax: (301) 772-8540
ciheagwara@unatek.com
Attention: Charles Iheagwara

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

Special Item Numbers

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

SIN 132-51 - INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES

FPDS Code D301	IT Facility Operation and Maintenance
FPDS Code D302	IT Systems Development Services
FPDS Code D306	IT Systems Analysis Services
FPDS Code D307	Automated Information Systems Design and Integration Services
FPDS Code D308	Programming Services
FPDS Code D308	Millennium Conversion Services (Y2K)
FPDS Code D310	IT Backup and Security Services
FPDS Code D311	IT Data Conversion Services
FPDS Code D313	Computer Aided Design/Computer Aided Manufacturing (CAD/CAM) Services
FPDS Code D316	IT Network Management Services
FPDS Code D317	Automated News Services, Data Services, or Other Information Services
FPDS Code D399	Other Information Technology Services, Not Elsewhere Classified (Desktop Management Information Assurance)

Contractor Information

Unatek, Inc.
1100 Mercantile Lane, Suite 115-A, Largo, MD 20774
(301) 583-4629
www.unatek.com

Contract Number: **GS-35F-0632T**

Period Covered by Contract: **September 11, 2007 – September 10, 2012**

This Authorized FSS IT Schedule Pricelist incorporates all modifications through P00001 dated _____.

General Services Administration
Federal Supply Service

Pricelist current through Modification #_____, dated _____.

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 OFFICES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS

SPECIAL NOTICE TO AGENCIES: Small Business Participation

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

For orders exceeding the micropurchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage!™ 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:

The 48 Contiguous states and the District of Columbia and Alaska, Hawaii and Puerto Rico.

2. Contractor's Ordering Address and Payment Information:

Order Address:
Unatek, Inc.
1100 Mercantile Lane,
Suite 115-A,
Largo, MD 20774
Phone: 301- 583-4629

Fax: 301-772-8540

Payment Address:
Unatek, Inc.
1100 Mercantile Lane,
Suite 115-A,
Largo, MD 20774
Phone: 301- 583-4629

Fax: 301-772-8540

3. LIABILIY FOR INJURY OR DAMAGE

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

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

Block 9: G. Order/Modification Under Federal Schedule
Block 16: Data Universal Numbering System (DUNS) Number: 003749132
Block 30: Type of Contractor – A. Small Disadvantage Business
Block 31: Woman-Owned Small Business - NO
Block 36: Contractor's Taxpayer Identification Number (TIN): 52-1984420

4a. **CAGE Code:** 4FEM7
4b. **Contractor has registered with the Central Contractor Registration Database.**

5. **FOB Destination** including Alaska, Hawaii and Puerto Rico.

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 Agreed upon between Unatek, Inc., and the ordering Agency.
132-51	As Agreed upon between Unatek, Inc., and the ordering Agency.

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

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

a. Prompt Payment: 0.5% – Net 15 days from receipt of invoice or date of acceptance, whichever is later.
b. Quantity- None
c. Dollar Volume- 1% for order over $300,000 for SIN 51 and over $20,000 for SIN 50
d. Government Educational Institutions- Same as discounts/pricing terms and conditions as all other government.
e. Other- none

8. **Trade Agreements Act of 1979, as amended:**

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

9. **Statement Concerning Availability of Export Packing:** Not applicable

10. **Small Requirements:** The minimum dollar value of orders to be issued is $100.00.

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

    A. The Maximum Order value for the following Special Item Numbers (SIN) is $500,000:

    Special Item Number 132-51 – Professional Services

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

    Special Item Number 132-50 –Training Courses

12. ORDERING PROCEEDURES FOR FEDERAL SUPPLY SCHEDULE CONTRACTS

[NOTE: Special ordering procedures have been established for Special Item Numbers (SINs) 132-51 IT Professional Services and 132-52 EC Services; refer to the terms and conditions for those SINs.]

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

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

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

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

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

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

information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301)975-2833.

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

(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 OFFICES:** Any ordering office, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the Government's convenience, and (m) Termination for Cause (See C.1.)

16. **GSA Advantage!**

GSA Advantage! is an 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 INCIDENTAL, NON-SCHEDULE ITEMS**

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

18. **CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS**

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

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

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

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

20. BLANKET PURCHASE AGREEMENTS (BPAs)

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:

Full details of 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 Government 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 Government's location, as agreed to by the Contractor and the Government.

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 Government.

4. CANCELLATION AND RESCHEDULING

a. The Government 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 Government to either cancel the order or reschedule the training at no additional charge. In the event the training class is rescheduled, the Government will modify its original training order to specify the time and date of the rescheduled training class.

b. In the event the Government fails to cancel or reschedule a training course within the time frame specified in paragraph a, above, the Government will be liable for the contracted dollar amount of the training course. The Contractor agrees to permit the Government 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 Government 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 Government, the Contractor must notify the Government 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 Government will be charged will be the Government training price in effect at the time of order placement, or the Government 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 Government 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 Government'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.

Government Per Diem Rate will be applicable.

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

Description of Information Assurance Classroom Seminars

Unatek offers on-site training as well as classes in our state of the art learning lab. Our instructors have extensive experience as both practitioners and trainers.

Seminars

- **Foundations of Intrusion Prevention: Effective Implementation Strategy**
- **Foundations of Web Application Security**
- **SOA, Web Services, and XML Security**
- **Intrusion Detection Systems**
- **Computer Forensics**
- **Project Management Foundations for Information Assurance Projects**

What's Included?

- **Expert Instruction** from our instructors with real-world experience.
- Guaranteed good class size, you get an intimate learning setting.
- All meals, snacks and refreshments included.
- Lecture, Lab Exercise and Text book
- CD-ROM with every tool and custom script used in course.

Foundations of Intrusion Prevention: Effective Implementation Strategy

Length: 1 day(s) course

Prerequisites:

- Understanding of the Windows Operating System
- Grasp the Linux Operating System or other Unix-based OS
- Understanding of the TCP/IP protocols
- Exposure to network reconnaissance and associated tools (nmap, nessus, netcat)
- Desire to learn about ethical hacking, and get great intrusion prevention training!

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

As the network landscapes have evolved from traditional client-server architectures to now include various platforms and components, including support for mobile, wireless and remote users, today's enterprise or corporate endpoint security must incorporate a multi-layer threat mitigation strategy that extends beyond application/circuit-level firewalls to include, not only intrusion detection systems but as well, intrusion prevention systems to secure remote access and provide zero-day protection.

The need for a multi-layer mitigation approach has become a mission-critical mandate to cope with the security challenges and advancements brought about by the dissolution of the traditional network perimeter, which have dramatically increased the opportunity for worms and viruses to propagate. Consequently, to better combat these evolving threats, enterprise and corporate network systems must look beyond traditional security architectures, which weren't designed for internal network security threats.

The latest technology in information security is Intrusion Prevention. Rather than relying on human intervention to respond to an attack, Intrusion Prevention Systems **automatically stops hackers, worms, and disgruntled employees before their attacks can complete.** This all happens before they can cause damage, potentially saving your organization millions.

Thus, Intrusion Prevention Systems (IPS) plays a crucial role as essential security components in combating not just external but internal threats for both wired and wireless (Wi-Fi) enterprise networks. They both enable comprehensive security monitoring and management capability
which makes them attractive as risk management tools and endears them to enterprises and organizations.

As with any new automated technology, there are many perils to avoid when implementing it. Just as Intrusion Prevention Systems can prevent hackers and worms, they can easily be configured incorrectly which can **block legitimate users from doing their jobs.** The intrusion prevention training you receive in this course will enable you to **deploy intrusion prevention systems safely.**

The Intrusion Prevention training offered by Unatek, Inc. covers all areas of intrusion prevention. **Host Intrusion Prevention and Network Intrusion Prevention** is covered in great detail.

Topics Covered Include:

- Understanding buffer overflows
- Anatomy of an exploit
- Network protocol based attacks
- Intrusion Prevention vs. Intrusion Detection
- Intrusion Prevention deployment strategies
- The stack and heap data structures
- The role the Kernel plays in attacks
- Linux, Solaris and Windows Kernels
- Unix system calls and the Windows API
- Vulnerability development and discovery
- Malicious worm internals
- Host Intrusion Prevention
- Syscall Interception
- Non-executable stacks/Non-executable heaps
- Page protection
- Heuristic and behavioral blocking
- Network Intrusion Prevention
- Web application IPS
- Layer 7 Intrusion Prevention
- Packet scrubbing
- Shunting and session sniping
- Attack signature development
- Mixed mode IPS
- DDoS Prevention
- Calculating ROI for Intrusion Prevention

Instructor-Led Hands-on Lab Exercises Include:

- Hack into an unprotected system
- Utilize a buffer overflow
- Implement a no-exec stack
- Attack a no-exec stack
- Implement an no-exec heap
- Attack a no-exec heap
- Syscall Redirection
- Implement page protection in Linux
- Page protection on Windows
- Page protection on OpenBSD
- Kernel hardening with PaX
- grsecurity Lockdown
- Use a stack canary
- Implement a Host Intrusion Prevention System
- Attempt two previous attacks against the Host
- Attempt two previous attacks against the Host Intrusion Prevention System
- Deploy Network Intrusion Prevention
- Capture an attack and write an IPS rule
- Build in web server layer 7 IPS
- Session sniping exercise
- Data correlation and multiple firewall blocking
- Shunting with routers

Foundations of Web Application Security

Length: 1 day(s) course

Prerequisites:

- An understanding of TCP/IP and OSI reference Models
- A basic understanding of networking

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

Most developers, IT professionals, and auditors learn what they know about application security on the job, usually by making mistakes. Application security is just not a part of many computer science curricula today and most organizations have not focused on instituting a culture that includes application security as a core part of their IT security efforts.

This powerful one day course focuses on the most common web application security problems, including the OWASP Top Ten. The course will introduce and demonstrate hacking techniques, illustrating how application vulnerabilities can be exploited so students really understand how to avoid introducing such vulnerabilities into their code.

This course starts with a module designed to raise awareness of just how insecure most web applications are. We demonstrate how easily hackers are able to attack web applications, and what some of the most common and most significant vulnerabilities are. The course then provides an overview of how web applications work from a security perspective.

The next modules detail a number of specific security areas. We describe common vulnerabilities, present best practices, and discuss recommended approaches for avoiding such vulnerabilities.

Topics Covered Include:

This course includes coverage of the following common vulnerability areas:

- Unvalidated Parameters *
- Broken Access Control *
- Broken Account and Session Management *
- Cross-Site Scripting (XSS) Flaws *
- Buffer Overflows *
- Command Injection Flaws *
- Error Handling Problems *
- Insecure Use of Cryptography *
- Denial of Service *
- Web and Application Server Misconfiguration *
- Poor Logging Practices
- Caching, Pooling, and Reuse Errors

- Code Quality

* The OWASP Top Ten Most Critical Web Application Vulnerabilities
For each area, the course covers the following:

- Theoretical foundations
- Recommended security policies
- Common pitfalls when implementing
- Details on historical exploits
- Best practices for implementation

Instructor-Led Hands-on Lab Exercises Include:

To cement the principles delivered via the lecture portion of the course, students can participate in a number of hands-on security testing exercises. During the hands-on exercises students will attack a live web application (i.e., WebGoat) that has been seeded with common web application vulnerabilities. The students will use proxy tools commonly used by the hacker community to complete the exercises.

Requirements

If you are interested in participating in the hands portion of the course, please bring a Windows based laptop that supports Java.

SOA, Web Services, and XML Security

Length: 1 day(s) course

Prerequisites:

- An understanding of TCP/IP and OSI reference Models
- A basic understanding of networking

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

The movement towards Web Services and Service Oriented architecture (SOA) paradigms requires new security paradigms to deal with new risks posed by these architectures. This session takes a pragmatic approach towards identifying Web Services security risks and selecting and applying countermeasures to the application, code, web servers, databases, application, and identity servers and related software.

Many enterprises are currently developing new Web Services and/or adding and acquiring Web Services functionality into existing applications -- now is the time to build security into the system!

Topics Covered Include:

Topics covered include understanding how web application risks (such as those in OWASP Guide and OWASP Top Ten) apply in a Web Services world, and Web Services security topics including:

- Web Services attack patterns
- Common XML attack patterns
- Data and XML security using WS-Security, SAML, XML Encryption and XML Digital Signature
- Identity services and federation with SAML and Liberty
- Hardening Web Services servers
- Input validation for Web Services
- Integrating Web Services securely with backend resources and applications using WS-Trust
- Secure Exception handling in Web Services

Understand the impact of Web 2.0 technologies like Ajax, and REST on distributed systems security.

Intrusion Detection Systems

Length: 3 day(s) course

Prerequisites:

- An understanding of TCP/IP and OSI reference Models
- A basic understanding of networking

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

This is a three-day interactive course where students will learn advanced functions of IDS and network intrusion management system.

The objective of the IDS training module is to maximize the return on your investment with hands-on and real world training on IDS network security products and technologies, security best practices and other IDS security service offerings.

Topics Covered Include:

Session 1: Overview

- General IDS Component Description

- General IDS Architecture
- Enterprise (High Level) Products Feature List

Session 11: Introduction to Network Security Threats

- Social Engineering
- Hacking: Internal vs. External
- Password Guessing
- Password Cracking (LC4)
- Password Policy Enforcement
- Sniffing & Spoofing
- Floods & DoS
- Trojans

Session 111: IDS Sensor Installation

- IDS Systems Requirements
- IDS Sensor Hardware Architecture
- IDS Topological Placement
- Console Functions
- Basic Sensor Connectivity Troubleshooting

Hands–on Lab

- Installation of Sensor software

Session IV: IDS Server Installation

- IDS Server Architecture
- IDS Systems Requirements
- IDS Topological Placement
- Server's OS Hardening
- Basic Server Connectivity Troubleshooting

Hands–on Lab

- Installation of Server software

Session 4: Graphical Interface Usage

- Architecture
- Viewing Alerts & Alert Filters
- Overview of Package vs. Backend (Sourcefire Sigs)
- Running Queries & Reports
- Configuring Packages_Backends
- Running Queries & Reports
- Configuring Alerts
- Configuring Space Management
- Diagnostics

Hands–on Lab

- Data Tuning Rules Examples

Session V: Advanced Server Topics

- Server File Architecture / Data Structure
- Failover CMS's
- Command Line Queries
- Troubleshooting Tools

Session VI: IDS Tuning

- Descriptions of key packages and backends
- Some Initial Suggested Tuning and Variable Configs

Hands–on Lab

- Lab: Catch the Hacker (replay Defcon traffic)

Session VII: Enterprise Console Installation

- System Reqs
- Preparing the Install Platform
- Step by step Install
- Post "install" configuration
- Connectivity Checks

Session VIII: EC Usage

- Viewing Alerts
- Filtering Alerts
- Customizing your view
- Saving your view
- Realtime Graphs
- Creating Correlators
- EC Administration functions
- Using Crystal Reports
- Customizing Crystal Reports

Computer Forensics

Length: 3 day(s) course

Prerequisites:

- Understanding of the Windows Operating System
- Grasp the Linux Operating System or other Unix-based OS
- Understanding of the TCP/IP protocols
- Exposure to network reconnaissance and associated tools (nmap, nessus, netcat)
- Desire to learn about ethical hacking, and get great intrusion prevention training!
- An understanding of TCP/IP and OSI reference Models
- A basic understanding of networking

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

The rise and growth of computer networks and rapid adaptation of their use in the work place has led to several issues related to all sorts of intrusion into network systems and in some cases cracking of standalone systems. As a result, incidents of break-ins abound and require that organizations respond with good incidence response and computer forensics program in place.

Given this, this course will discuss computer forensics and incidence response in the enterprise.

***Topics Covered Include*:**

- Fundamentals of Computer Forensics
- Legal and Ethical issues related to Computer Forensics
- Best practices and tips for gathering evidence in a secure fashion
- Investigating attacks on Windows and Linux Machines
- Evidence Collection from portable digital devices (i.e. iPods, PDAs, Cell Phones)
- Incidence Response best practices
- Encase, Autopsy and other tools

Project Management Foundations for Information Assurance Projects

Length: 2 day(s)

Prerequisites:

Minimum and maximum number of students per class: 5 - 30

Locations: 1100 Mercantile Lane, Suite 115-A, Largo, MD 20774

Class schedules: Updated on the Websites: www.unatekconference.com; www.intrusiononline.net

Course Times: Each class begins at 8:30 AM and runs until 5 PM.

Description:

The effective project manager must be able to develop strategies, work plans, estimates and schedules and monitor progress against them in today's dynamic market. Simply planning a successful project is merely half the job: attentive tracking, status reporting and change management are all needed to ensure success. This 3-day workshop blends five modules from our Project Management curriculum. It provides practical tools and techniques for planning and managing the variables or constraints of project success, using content discussion, a series of exercises and a project simulation application. Participants gain classroom experience with today's best practices for structuring, estimating, scheduling and tracking projects, in order to bring them in on time, within budget and with high quality.

Topics covered Include:

Introduction & Concepts Module

- Definition of a Project; PMI & PMBOK Knowledge Areas:
- Historical Project Problems; The Project Variables
- Project Management Skills; Project Processes; Initial vs. Detailed Planning Process

Organizing Module

- Rapid Planning; Project Kick-Off; Team Organization, Roles & Responsibilities; Infrastructure
- The Project Office; Background Analysis; Project Requirements; Scope & Objectives
- Initial Project Forecasts; Cost/Benefits Analysis; Prioritization; Project Manager Activities
- Project Strategies; Lifecycles; Deliverables; Risk Management; The Project Charter.

Structuring Module

- Phase Initiation Process; Work Breakdown Structures; Decomposition and Templates;
- Identifying Work Packages; Phase Organization; Assigning resources to the tasks
- Delegation; Quality Assurance; and the Project Plan.

Task Estimating Module

- Determining the Estimating Approach; Definitions; Estimating Effort; Simple Estimating
- Delphi Estimating; Modified PERT Estimating; Statistical Processes; Conversion to Duration
- Documenting the Task Estimate; Contingency & Reserves Planning
- Estimating Project Management Effort;

Scheduling Module

- Terminology and Graphical Techniques
- Network Diagrams & Critical Path Determination; Precedence Analysis
- Gantt Charts; Resource Leveling; Histograms
- Milestones & Baselines; Performing the Visibility Review;
- The Planning, Estimating and Scheduling Process Steps

Tracking & Controlling Module

- The Tracking Information; Executing & Controlling Processes
- Tracking Methods Analysis & Guidelines; Earned Value
- Determining Status and Reforecasting the Project Schedule
- Project Reporting; Change Management
- Completing the Phase; Project Completion Criteria; Workshop to Workplace Transition.

Topics Covered Include:

Rapid Planning:

- Organizing: Perform Rapid Planning: including identification of the project variables; definition of the project scope and preliminary requirements; early forecasts of effort, duration and staffing; cost/benefit analysis; team roles & responsibilities; risk management; project strategies and the creation of a project charter.

Phase Planning:

- Structuring: Identify and structure the tasks of a phase into work packages; organize the project team; apply resources to the plan; delegate tasks to the team members; build in Quality Assurance Reviews and create the Project Plan.
- Task Estimating: Improve task estimates by determining the appropriate estimating approach; estimating effort and duration; effectively document task assumptions;
  Padding vs. Contingency and estimating Project Management effort.
- Scheduling: Define the scheduling terminology; develop network diagrams; determine Critical Path and perform Precedence Analysis to reduce the overall project duration. Develop Gantt charts and perform resource leveling; identify milestones and establish the project baseline.
- Tracking & Controlling: Identify the minimum effort tracking mechanisms appropriate for the project; re-forecast the project schedule and update the project plan; determine the reporting processes; manage the change process and complete the phase and project.

AUTHORIZED GSA FSS TRAINING SCHEDULE PRICELIST

Course	Duration (Days)	Price/Rate (Onsite/Offsite)
Foundations of Intrusion Prevention: Effective Implementation Strategy	1	$$736.25
Foundations of Web Application Security	1	$612.75
SOA, Web Services, and XML Security	1	$612.75
Intrusion Detection Systems	3	$1890.5
Computer Forensics	3	$1890.5
Project Management Foundations for Information Assurance Projects	2	$591.55

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

1. **SCOPE**

a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services and Special Item Number 132-52 Electronic Commerce Services apply exclusively to 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 office.

2. **PERFORMANCE INCENTIVES**

a. When using a performance based statement of work, performance incentives may be agreed upon between the Contractor and the ordering office on individual fixed price orders or Blanket Purchase Agreements, for fixed price tasks, under this contract in accordance with this clause.

b. The ordering office must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.

c. To the maximum extent practicable, ordering offices shall consider establishing incentives where performance is critical to the agency's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. **ORDER**

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

b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. **PERFORMANCE OF SERVICES**

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

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

c. The Agency should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

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

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

(1) Cancel the stop-work order; or

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

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

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

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

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

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

6. **INSPECTION OF SERVICES**

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

7. **RESPONSIBILITIES OF THE CONTRACTOR**

The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY

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

9. **INDEPENDENT CONTRACTOR**

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

10. ORGANIZATIONAL CONFLICTS OF INTEREST

a. Definitions.

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

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

An "Organizational conflict of interest" exists when the nature of the work to be performed under a proposed Government contract, without some restriction on activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor's or its affiliates' objectivity in performing contract work.

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

11. INVOICES

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

12. PAYMENTS

For firm-fixed price orders the Government shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts (Alternate I (APR 1984)) at FAR 52.232-7 applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts (FEB 1997) (Alternate II (JAN 1986)) at FAR 52.232-7 applies to labor-hour orders placed under this contract.

13. RESUMES

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

14. INCIDENTAL SUPPORT COSTS

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

15. APPROVAL OF SUBCONTRACTS

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

16. **DESCRIPTION OF IT SERVICES AND PRICING**

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

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

The following is an example of the manner in which the description of a commercial job title should be presented:

Commercial Labor Category	Min Experience	Education	Functions
Senior Program Director	12 years of IT or Management experience	Masters Degree in Computer Science, MIS or Management, PMP or equivalent	Manages very large and complex programs and projects, involving large budget, enterprise, multi-agency or multi-organization coordination. Possesses and demonstrates advanced knowledge of Project Management areas, such as, Project frameworks, budgeting and estimating, strategic planning, lifecycle selection, portfolio management, enterprise resource management, PMO establishment, contractor management, mentoring and instruction. Able to coordinate and facilitate meetings and strategy planning sessions involving senior and executive management. Supervises project managers and develops integrated program reports suitable for senior and executive management review. Develops project management curriculums and mentors stakeholders and managers. Implements and manages enterprise project schedules using a variety of COTS tools, such as, Primavera and MS-Project. Possesses Project Management Professional, equivalent certification or training in Project Management.
Principal Engineer	10 years of IT experience	Bachelor's Degree in Computer Science, MIS or Management or equivalent.	Provides technical management of software development process. Interprets business requirements and creates system architectures models for client/server web or N-Tier environments. Supervisor of technical design teams and uses a variety of case tools and Integrated Development environment to promote efficiency. Supports the Project Manager with activities definition, technical planning and end user meetings. Mentor team members. Has developed complex reusable module and codes
Project Manager	10 year of IT experience required	Bachelor's Degree in Management or equivalent.	Develops and manages project plans, schedules and status reports. Ensures the works is done in a timely manner with high quality. Consults with customers, users and leads integrated product teams. Supervises team members on a daily basis and reviews team status report.
Information Security Consultant	Minimum 8 years of experience required	Bachelor's degree in Computer Science, Information Systems or equivalent.	Possesses advanced level knowledge and experience in information security and/or relevant information technology best practices and standards with a heavy concentration on solving customer security challenges. Performs project tasks with little or no supervision. Leads teams on large scale projects. Contributes a significant piece of a project deliverable. Possess ability to create detailed, professional documentation to be delivered to client and is able to create and recommend remediation for components of security policies. Provides specific recommendations for a clients business or technical issues. (Example: Lack of or enforcement of a password policy.). Understands one or more regulatory areas including, but not limited to: PCI (Visa CISP, MasterCard SDP, Discover DISC, and Amex DSOP), ISO 17799/BS 7799, GLBA, HIPAA, and SOX. Understands the creation, management, and oversight of Information Security Programs, Business Continuity Planning and Change Control functions for Information Services. Familiarity with retail information security challenges.
Subject Matter Expert	Minimum 10 years of experience required	Master's degree in Computer Science, Information Systems or equivalent with min 5+	Across all topics, Subject Matter Expert should have expertise on security-related topics such as authentication mechanisms, data protection, validation checking, encryption, hashing, principle of least privilege, software attack methodologies,

		yrs relevant work experience in high-paced, IT enterprise security environment.	physical security, social engineering, etc. across the variety of platforms. Leads architectural design and review sessions with IT teams to ensure that security is incorporated into projects at the earliest stages by identifying potential risks and threats as well as mitigating designs or controls. Provides specific IT security engineering expertise into tactical project tasks. Such areas might include securing databases, implementing encryption, configuring wireless networks, etc. Helps identify areas of infrastructure the Firm might want to invest in to further improve the discipline of IT security. This could include commercial tools, internally developed libraries, certification courses, and so forth.
Information Security Trainer	Minimum 10 years of experience required	Master's degree in Computer Science, Information Systems or equivalent. Doctorate degrees preferred with current industry certifications	Prepares the program structure, course outline and syllabus for information security training. Conducts training sessions. Organizes laboratory, demo or practical exercises using case studies. Facilitates interactive learning sessions. Assigns and grades tests, quizzes and examinations. Documents results. Provides inputs on how to improve student performance and course content and structure. Assists with the preparation of training materials and publications in select editions. Makes recommendations on the overall strategy for information security educational outreach programs.
Incident Response Engineer/Coordinator	Minimum 4 years of experience required in the areas of Information Security and Information Technology. Incident Response experience required	Bachelor's degree in Computer Science, Information Systems/Risk Management or equivalent.	Incident Response Engineer works closely with Information Technology Department to help in the coordination effort to remediate security alerts and respond to information security related incidents that could potentially impact the network, systems and applications. Responsible for performing the daily tasks associated with information security, incident response and handling, vulnerability handling and security event monitoring. Designs & implements a security event mgmt program including IT/IS incidents to gather, store, correlate, analyze and respond to security data from logs & incident reports. Performs forensics investigations of security incidents. Conducts application security reviews to ensure proper security controls are implemented. Performs monitoring/auditing activities (e.g. monitoring access logs and assigned privilege levels) and respond to security events as appropriate. Executes vulnerability tests on networks, systems and applications when necessary. Performs regular scans and security assessments of the infrastructure, notify/escalate with IT, and document findings in a complete comprehensive report that includes technical and non-technical findings and recommendations.
Senior Information Security Engineer	Minimum 8 years of experience required in information security, risk management and/or auditing. Current professional certification(s) in security and/or auditing preferred (e.g., CISM, CISSP, CISA, GIAC, etc).	Bachelor's or Master's degree in Computer Science, Information Systems, Risk Management, Telecommunications or equivalent+t.	Under the Supervision of a Program Manager or Director. Able to provide day-to-day IT security expertise for multiple projects without supervision. Provide technical team management for Information Security Engineers. Acts as a bridge between senior program/project management and the technical team. Duties include supervising IT security team, developing and maintaining security rules and providing security training to ISO staff as needed; installing, configuring and maintaining the security infrastructure (RSA servers, Firewalls, IDS, VPN); and managing vendor relationships. Assesses security risks, identifies and recommends effective solutions, and consults with operations or business units when necessary. Improves security infrastructure through internal assessments, identification of vulnerabilities, and managing corrective actions. Identifies and

			implements missing key security program elements such as security policies, standards, guidelines, patch policy, Computer Incident Response Team procedures. Design the architecture of the Information Assurance system, working closely with the Program Security Manager, Systems Engineering, and Software Engineering to synthesize security requirements into systems which can be certified and which meet customer requirements. Implements IT Security Architecture and set all policies and procedures. Interfaces with business units to understand the risks and address their needs. Compares new Security Architectures to NIST, ISO 17799, etc. Assists with the investigation of security breaches and assist with disciplinary and legal matters associated with such breaches as necessary. Works effectively across a large information security team, understanding the larger team's role (network, platform and monitoring) in the overall security strategy of the firm.
Information Security Engineer	Minimum 5 years of experience required	Bachelor's degree in Computer Science, Information Systems, Telecommunications or equivalent.	Under the Supervision of a Senior Security Engineer. Provides day-to-day IT security expertise for multiple projects. Duties include developing and maintaining security rules and providing security training to ISO staff as needed; installing, configuring and maintaining the security infrastructure (RSA servers, Firewalls, IDS, VPN); and managing vendor relationships. Performs risk assessments and security testing as part of a security engineering team. Analyzes system security on a variety of information systems, network devices (firewalls, routers, and switches), web server and database applications. Supports the certification and accreditation process for IT systems and networks including preparation of key documentation and planning and conducting security tests and evaluations, analytical and systems engineering for development of strategic plans and security architectures for government activities. Develops and/or analyzes information systems security requirements. Consult with the application development teams on application security requirements, including key SMD applications that use single sign-on and common database(s), analyze potential security problems and take appropriate corrective action. Supports adapting, interpreting, and/or developing INFOSEC policy; performing site security compliance reviews and site surveys; and providing security awareness training. Will participate and perform compliance reviews of field activities.
Risk Assessment/Analyst Engineer	5 years of IT experience performing requirements analysis, design and remediation	Bachelor's Degree in Management or Computer Science or equivalent.	Under supervision, analyzes security risks inherent in Hardware, Software and Communication systems. Assesses security risks, identifies and recommends effective solutions, and consults with operations or business units when necessary. Identifies and implements missing key security program elements such as security policies, standards, guidelines, patch policy, Computer Incident Response Team procedures. Analyzes user requirements designs and security elements of an application. Assists in preparation of requirements and design documents. Able to analyze data and object models security risks. Facilitate and documents software requirements. Perform risk analysis of network and application systems using a variety of Risk Assessment tools. Communicates technical information to team members and end-users. Designs systems amd network security remediation to meet analysis requirements. Establishes rapport

			with customer security organizations and communicate and translate requirements to find best fit solutions for customers. Performs and updates impact analysis reports for customer specified requirements against system architecture/design. Participates in the Test Program to ensure that security controls are properly planned and implemented. Evaluates changes to system software or hardware for impact to security.
Comp/Telecom Security Specialist	Minimum 3 years of experience required	Bachelor's degree in Computer Science, Information Systems, Telecommunications or equivalent certifications.	Under the Supervision of a Project Manager. Participates in a team responsible for the day to day performance, availability and reporting of a network infrastructure and computing environment. This professional will perform and handle the following. Implements network changes as needed. Measuring and monitoring the health and performance of the network infrastructure, which supports e-commerce. Produce daily, weekly and monthly performance reports. Continually enhances and develops the reporting and monitoring tools. Documents configurations, policies and procedures relative to network infrastructure. Makes recommendations on architectural improvements leading to better performance and availability. Strategize and work with other IT groups to ensure coordination of efforts and consistent architectural designs. Possesses practical business experience supporting Internet network infrastructure with firewall technology, switches, virus protection, help desk services and routers.
Project Administrator	4 years of IT experience	Bachelor's Degree in Computer Science or MIS or Management or equivalent.	Monitors work in progress with Project Manager throughout the project management lifecycle. Monitors project team activities to ensure project objectives are met within established time frames and budgets. Follow up on deliverables and deliverable dates. Track deliverables and slippages and inform the Project Manager, Sponsor, Lead and/or Director of the status of all project activities. Maintain, monitor, and revise project schedules, document all aspects of assigned projects.
Technical Manager	10 year of IT experience required	Masters Degree in Computer Science, Management or equivalent.	Develops and formulates solutions to Information Technology Security problems. Supports project managers in requirements engineering, scope definition, technical approach, and execution development plans. Supervises and mentors teams of engineers, programmers and analysts. Has responsibility for completion of technical tasks in a timely fashion with desired quality and monitoring the work of others. Supports the Project Manager in schedule development, task identification and reporting as required. Responsible for task, resource and skill identification and estimates of effort. Has advanced knowledge of software security architecture, network security, cyber security, software development lifecycles, object oriented architecture, Java, C++, or XML programming, e-Commerce and process frameworks, such as, CMM, ISO or PMBOK. Models and design advanced integrated architectures using Case Tools, such as, Rational Rose, Erwin in n-Tier, Legacy or Client/server environments.
Technical Lead	8 years of IT experience	Bachelors Degree in Computer Science, MIS, or equivalent	Responsible for defining the technical approach and development strategy for technology projects. Meets with end users and developers to capture requirements and define the scope of projects. Prepares requirements and design specification documentation. Recommend development strategies which take into account the requirements, operating system, hardware and software constraints. Proficient in a variety of security tools. Advanced knowledge and use of Case

			Tools, e-Business, Software Security Architectures, Quality Assurance and Project LifeCycles. Provides technical guidance and support to team members.
Configuration Manager	8 years of IT experience	Bachelor's Degree in Computer Science or MIS or equivalent.	Provide project level support including compiling the necessary procedures, policies and processes for establishing and maintaining integrity in software baselines. Document standard configuration management processes and procedures to include: version control, build and release management, SCM audit reports, configuration identification and control, software product baselines, change management, tracking and reporting in a controlled and methodical SCM environment.
Configuration Management Analyst	6 years of IT experience	Bachelors Degree in Computer Science, MIS or equivalent	Under supervision documents processes and procedure necessary for maintaining and managing configuration status of Hardware and Software. Identifies Configuration Items to be placed under Configuration Management, tracks Change Request and Build Versions, which change the state of the software under Configuration Control. Provides Project Management and Team Members with status reports and participates in Configuration Control Board meetings. Installs, configures and manages Configuration Management tools, such as, Rational ClearQuest, ClearCase and Merant PVCS.
Junior Project Manager	Minimum 5 years of demonstrated experience.	Bachelor's degree in Management or equivalent.	Under the Supervision of a Program Director or Program Manager. Prepares project schedules, project plans, issues, risk reports, WBS, cost/benefit analyses and status reports. Supervises the activities of a project team and ensures that the work is performed in a timely manner with desired quality. Is knowledgeable and able to perform resource management, earned value analysis and critical chain management. Has advanced knowledge of MS-Project and/or other project management tools. Consults with Senior Managers, customers and stakeholders to ensure that project goals are aligned with the company's objectives.
IT Security QA Analyst	Minimum 3 years of experience required	Bachelor's degree in Computer Science, Information Systems or equivalent.	Under the Supervision of a Project Manager or Technical Manager. Supports the internal process of risk assessment across the IT control environments. Interfaces with IT Administrative, Project Management and technical staff to ensure the successful release of deliverables. Determines cross-functional issues that arise during the planning of production implementation releases, and supports the resolution of these issues. Participates as a resource in system development projects to ensure proper egress from the data collection environment into the QA environment; the data collected in QA and development of assessment plans to be executed by the project manager. Prepares reports and ensures that key disciplines (such as daily version check-ins) are performed. Knowledgeable in QA processing, change management disciplines and software development methodologies.
Senior Programmer Analyst	7 years of IT experience performing requirements analysis, design and programming	Bachelor's Degree in Management or Computer Science or equivalent.	Facilitate and documents software requirements, perform Object Modeling and Database Modeling using tools such as Rational Rose and ERwin Communicates technical information to team members and end-users. Designs and codes software to meet software requirements using Java, C++, PowerBuilder, XML and other languages.
Programmer Analyst	3 years of IT experience performing	Bachelor's Degree in Management or Computer Science or	Under supervision, analyzes end user requirements designs and codes elements of an application. Assists in preparation of requirements and design documents. Able to analyze data and

	requirements analysis and programming.	equivalent.	object models created in Case tools, such as, Erwin and Rational Rose. Programs in a variety of programming languages – Java, C++, and ColdFusion. Document code design, develops test cases for unit testing, debugs and comments source code. Creates and modifies database tables needed for application development under direction of a DBA.
Database Administrator	8 years of IT experience	Bachelors Degree in Computer Science, MIS or equivalent	Performs all activities needed for reliable and efficient operation of complex database software, such as, Oracle, MS-SQL Server and Informix. Uses Erwin or other Case tools to model design and manage databases. Mentors junior database analyst, performs complex queries and tunes production databases. Supports the Program Manager with database planning and status reporting activities. Assess the performance, design implications and production impact of all requested database changes. Provides cost and schedule impact analysis to Project Manager.
Security Architect	8 years of IT experience	Bachelors Degree in Computer Science, MIS or equivalent	The Security Architect II is expected to be an expert in a broad range of security disciplines and must be well versed in a broad spectrum of technology areas. The Security Architect is responsible for leading the development of security technology plans/roadmaps that address current state challenges and how to achieve a target future state. The Security Architect may also participate as a Solution Architect for high priority, strategic IT security projects. In addition, this role will lead security technology evaluation and selection activities and will define and develop security services, standards, reference architectures, assets and frameworks required to support T-Mobiles business strategy. The Security Architect will serve as point of escalation, review and approval for key issues, significant security projects and decisions.
Help Desk Manager	Minimum 7 years of experience in the IT field.	Requires a bachelor's degree in Computer Science, MIS or equivalent .	Manages a team of support personnel who troubleshoot IT issues. Implements policies and procedures regarding how problems are identified, received, documented, distributed, and corrected. Ensures maximum issue resolutions in minimum time. Evaluates new information systems products or services and suggests changes to existing products or services to better aide the end user. Familiar with a variety of the field's concepts, practices, and procedures. Relies on extensive experience and judgment to plan and accomplish goals. Performs a variety of tasks. Leads and directs the work of others. A wide degree of creativity and latitude is expected. Typically reports to head of a unit/department.
Help Desk Specialist	Minimum of 3 years of Helpdesk experience.	Associate's degree plus preferred certifications in A+ and MCP is a plus.	Analyze, resolve, and troubleshoot technical problems by phone, email, remotely, and on-site. Able to support executive level users.. Ensures maximum issue resolutions in minimum time. Must exhibit strong analytical and customer service skills. Uses general knowledge of hardware and software components to resolve systems problems. Knowledge of Windows & Unix operating systems strongly preferred. Basic networking principles, LAN, dial up networking, PCPIP and RAS configurations strongly preferred.

AUTHORIZED GSA FSS IT SCHEDULE PRICELIST

Job/Title:	**GSA Price/Rate (Onsite/Offsite)**
1. Senior Program Director	$190.00 per hour
2. Principal Engineer	$133.00 per hour
3. Project Manager	$123.50 per hour
4. Project Administrator	$95.00 per hour
5. Technical Manager	$114.00 per hour
6. Technical Lead	$104.50 per hour
7. Subject Matter Expert	$296.87 per hour
8. IT Security Trainer	$296.87 per hour
9. Senior Information Security Engineer	$118.75 per hour
10. Information Security Engineer	$95.00 per hour
11. Information Security Consultant	$114.00 per hour
12. Risk Assessment /Analyst Engineer	$104.50 per hour
13. Security Architect	$ 109.25 per hour
14. Configuration Manager	$104.50 per hour
15. Configuration Management Analyst	$99.75 per hour
16. Senior Programmer Analyst	$95.00 per hour
17. Programmer Analyst	$85.50 per hour
18. Database Administrator	$114.00 per hour
19. Junior Project Manager	$95.00 per hour
20. IT QA Analyst	$44.17 per hour
21. Comp/Telecom Security Specialist	$61.75 per hour
22. Help Desk Manager	$80.75 per hour
23 Help Desk Specialist	$61.75 per hour
24. Incident Response Engineer	$90.25 per hour

USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

Aligned Development Strategies, Inc. provides commercial products and services to the Federal Government. 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 demonstrates 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 Federal Government contracts. To accelerate potential opportunities please contact **Charles Iheagwara, Ph: (301) 583-4629, ciheagwara@unatek.com, Fax: (301) 772-8540**

BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE

(Insert Customer Name)

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

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

Signatures

Agency	Date	Contractor	Date

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 Agency):

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

MODEL NUMBER/PART NUMBER	*SPECIAL BPA DISCOUNT/PRICE

(2) Delivery:

DESTINATION	DELIVERY SCHEDULES / DATES

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

(4) This BPA does not obligate any funds.

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

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

OFFICE	POINT OF CONTACT

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

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

(a) Name of Contractor;

(b) Contract Number;

(c) BPA Number;

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

(e) Purchase Order Number;

(f) Date of Purchase;

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

(h) Date of Shipment.

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

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

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 agency 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.