ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 31

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO. NRC-33-01-191

1. DATE OF ORDER: 09-15-2004
2. CONTRACT NO. (If any): GS35F0079J
3. ORDER NO.: 010 MODIFICATION NO.:
4. REQUISITION/REFERENCE NO.: NSIR-04-539
5. ISSUING OFFICE (Address correspondence to):
U.S. Nuclear Regulatory Commission
Div of Contracts CMC#1
Two White Flint North - MS T-7-I-2
Washington, DC 20555-0001

6. SHIP TO:
a. NAME OF CONSIGNEE: U.S. Nuclear Regulatory Commission
b. STREET ADDRESS:
c. CITY: Washington
d. STATE: DC
e. ZIP CODE: 20555-0001
f. SHIP VIA:

7. TO:
a. NAME OF CONTRACTOR: ALLIED TECHNOLOGY GROUP INC
b. COMPANY NAME:
c. STREET ADDRESS: 1803 RESEARCH BLVD STE 601
d. CITY: ROCKVILLE
e. STATE: MD
f. ZIP CODE: 208503167

8. TYPE OF ORDER
[ ] a. PURCHASE ORDER
Reference your _____
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

[X] b. DELIVERY/TASK ORDER
Except for billing instructions on the reverse, this delivery/task order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page $18,452.56
B&R:411-15-131-398, JOB CODE: R1138, BOC: 2572
APPN. NO.: 31X0200.411

10. REQUISITIONING OFFICE NSR
Clarissa L. Evans Brown - T-4L7

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
[X] a. SMALL [ ] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [ ] d. WOMEN-OWNED

12. F.O.B. POINT: Destination
14. GOVERNMENT B/L NO.:
15. DELIVER TO F.O.B. POINT ON OR BEFORE: See schedule.
16. DISCOUNT TERMS: N/A

13. PLACE OF
a. INSPECTION: Destination
b. ACCEPTANCE: Destination

FOR INFORMATION CALL: (No collect calls)
Donald King
301 415 6731

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The U. S. Nuclear Regulatory Commission (NRC) hereby accepts the quotation of Allied Technology Group, Inc. (Allied) dated July 1, 2004, which is hereby incorporated by reference and made a part hereof this delivery order, to provide the NRC with computer security services for its Computer Security Services to the NRC NSIR for OCIMS, ERDS, and DTS, at the firm fixed unit price reflected in the Schedule of Prices/Costs for each task. TIN: 52-1603280 DUNS NO.: 62-122-5598 NRC Project Officer: Clarissa L Evans Brown (301) 415-6891		See CONTINUATION Page			

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.
SUBTOTAL

21. MAIL INVOICE TO:
a. NAME: U.S. Nuclear Regulatory Commission
Payment Team, Mail Stop T-7- I-2
b. STREET ADDRESS (or P.O. Box): Attn: (insert contract or order number)
c. CITY: Washington
d. STATE: DC
e. ZIP CODE: 20555-0001

SEE BILLING INSTRUCTIONS ON REVERSE

17(h) TOTAL (Cont. pages)

17(i). GRAND TOTAL $18,452.56

22. UNITED STATES OF AMERICA BY (Signature): Donald A. King

23. NAME (Typed): Donald A. King
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

TEMPLATE - ADM001

ADM002

SUPPLEMENTAL INVOICING INFORMATION

If desired, this order (or copy thereof) may be used by the Contractor as the Contractor's invoice, instead of a separate invoice, provided the following statement, (signed and dated) is on (or attached to) the order: "Payment is requested in the amount of $_____. No other invoice will be submitted." However, if the Contractor wishes to submit an invoice, the following information must be provided: contract number (if any), order number, item number(s), description of supplies or services, sizes, quantities, unit prices, and extended totals. Prepaid shipping costs will be indicated as a separate item on the invoice. Where shipping costs exceed $10 (except for parcel post), the billing must be supported by a bill of lading or receipt. When several orders are invoiced to an ordering activity during the same billing period, consolidated periodic billings are encouraged.

RECEIVING REPORT

Quantity in the "Quantity Accepted" column on the face of this order has been: ☐ inspected, ☐ accepted, ☐ received by me and conforms to contract. Items listed below have been rejected for the reasons indicated.

SHIPMENT NUMBER	PARTIAL / FINAL		DATE RECEIVED	SIGNATURE OF AUTHORIZED U.S. GOVT REP.	DATE
TOTAL CONTAINERS		GROSS WEIGHT	RECEIVED AT	TITLE	

REPORT OF REJECTIONS

ITEM NO.	SUPPLIES OR SERVICES	UNIT	QUANTITY REJECTED	REASON FOR REJECTION

A.1 SEAT BELTS

Contractors, subcontractors, and grantees, are encouraged to adopt and enforce on-the-job seat belt policies and programs for their employees when operating company-owned, rented, or personally owned vehicles.

NRC-33-01-191-010 SECTION B

SCHEDULE OF SERVICES

CLIN 0001 -TASK 2.2.0 Attend Orientation Meeting

Labor Category	Labor Rate	Estimated Hours	Estimated Price
Project Manager 206C	[redacted]		$469.12
Sr. Systems Analyst 205C	[redacted]		$312.76
Subtotal		[redacted]	$781.88

CLIN 0002 -TASK 2.2.1 Develop Security Test & Evaluation Plan

Labor Category	Labor Rate	Estimated Hours	Estimated Price
Project Manager 206C	[redacted]		$938.24
Sr. Systems Analyst 205C	[redacted]		$3,127.60
Sr. Systems Analyst 205C	[redacted]		$625.52
Subtotal		[redacted]	$4,691.36

CLIN 0003 - TASK 2.2.2 Conduct Security Test & Evaluation and Prepare Report

Labor Category	Labor Rate	Estimated Hours	Estimated Price
Project Manager 206C	[redacted]		$1,876.48
Sr. Systems Analyst 205C	[redacted]		$2,189.32
Sr. Systems Analyst 205C	[redacted]		$2,502.08
Subtotal		[redacted]	$6,567.88

CLIN 0004 - TASK 2.2.3 Prepare Re-certification/Re-Accreditation Report

Labor Category	Labor Rate	Estimated Hours	Estimated Price
Project Manager 206C	[redacted]	[redacted]	$2,814.72
Sr. Systems Analyst 205C	[redacted]	[redacted]	$1,876.56
Sr. Systems Analyst 205C	[redacted]	[redacted]	$625.52
Subtotal		[redacted]	$5,316.80

CLIN 0005 - TASK 2.2.4 Prepare and Conduct Exit Briefing

Labor Category	Labor Rate	Estimated Hours	Estimated Price
Project Manager 206C	[redacted]	[redacted]	$469.12
Sr. Systems Analyst 205C	[redacted]	[redacted]	$625.52
Subtotal		[redacted]	$1,094.64

TOTAL ALL TASKS **$18,452.56**

The fixed unit price of each line item shown above to meet requirements as delineated in Section entitled "Statement of Work," shall include all cost deemed necessary by the offeror.

B.2 CONSIDERATION AND OBLIGATION

(a) The total estimated amount of this contract(ceiling) for the products/services ordered, delivered, and accepted under this contract is **$18,452.56**. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this contract.

CONTINUATION PAGE

B.1 SCHEDULE OF SUPPLIES OR SERVICES AND PRICE/COSTS

1 PROJECT TITLE

The title of this project is as follows:

"COMPUTER SECURITY SERVICES TO THE NRC OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE OPERATIONS OCIMS, ERDS, AND ETS"

2. BRIEF DESCRIPTION OF WORK

a) Brief description of work:

The U.S. Nuclear Regulatory Commission requires contractor support to provide: (1) develop a Project Management Plan; (2) develop Security Test and Evaluation Plan; (3) conduct ST and E and Prepare Report; (4) Prepare Re-certification/Re-Accrediation Reprot; and (5) develop an Exit Briefing; for the NRC Office of Nuclear Security and Incident Response.

(b) Only Contracting Officers of the NRC or other individuals specifically authorized under this task order may authorize the initiation of work under this task order. The provisions of this task order shall govern all required work hereunder.

3. SCHEDULE

The Contractor shall provide **computer security services** support services to NRC in accordance with the "DESCRIPTION/SPECIFICATIONS/WORK STATEMENT" for the task order period of performance at the rates as set forth below.

(b) The amount presently obligated with respect to this contract is **$18,452.56**. The Contracting Officer may issue orders for work up to the amount presently obligated. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

B .3 PERIOD OF PERFORMANCE

This order shall be effective from July 27, 2004, through September 30, 2004.

B.4 TABLE OF DELIVERABLES AND SCHEDULE OF DELIVERY

Deliverables and due dates are summarized in the table below. Deliverable due dates are based on workdays: Each deliverable line in this schedule of deliverables table has two (2) appended columns: "T+#" gives the number of expected work days required for the line items completion from project award date.

"Required date" maximum completion dates already determined by NSIR.

Deliverable #	Milestone #	Deliverable Title	T+#	Required Date
		Orientation Meeting	-	With 5 days of task award.
1	1	Security Test & Evaluation (ST&E) Plan	T+10	
2	2	Security Test & Evaluation (ST&E) Report	T+20	
3	3	Prepare the Re-certification/Re-accreditation Report	T+25	
3	4	Exit Briefing	T+25	

4.4 Instructions for Deliverables

Deliverables shall be delivered on the dates specified in the task order. If for any reason a deliverable cannot be delivered within the scheduled time frame, the Contractor shall notify the NRC Contracting Officer and NRC Project Officer in writing with cause of delay and the proposed revised schedule. This notice shall include the impact on the overall project. The NRC Project Officer shall make a business decision about the impact of the delay and forward the impact to the Contracting Officer.

Each deliverable shall first be submitted in draft for NRC review. NRC shall have 5 working days to review each draft deliverable and respond with comments or approval. Upon approval by NRC of the original draft or the corrected draft, the deliverable shall be delivered in final form to the NRC Project Officer and NRC Contracting Officer. For each deliverable (draft or final), the Contractor shall provide one (1) hard copy and one (1) electronic version of the deliverable to the NRC Project Manager, unless otherwise indicated. All deliverables shall be formatted and prepared using Corel WordPerfect software for the documentation and reports, and Microsoft Powerpoint for the briefings. All written deliverables shall be phrased in language that can be understood by the non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

4.4 Place for Deliveries

All correspondence and reports related to this Task Order, inclusive of the deliverables, shall be delivered to the CO and PO at the following locations:

Nuclear Regulatory Commission
ATTN.: Contracting Officer: Donald A. King
NRC Task Order#: NRC-33-01-191-010
Two White Flint North, Mail Stop: T7 I 2
11545 Rockville Pike
Rockville, MD 20852-2738

Nuclear Regulatory Commission
ATTN: Project Officer: Clarissa L. Evans Brown
NRC Task Order#: NRC-33-01-191-010
Two White Flint North, Mail Stop: T4L7
11545 Rockville Pike
Rockville, MD 20852-2738

C. STATEMENT OF WORK - COMPUTER SECURITY SERVICES TO THE NRC NSIR for OCIMS, ERDS and ETS

1.0 BACKGROUND

The Contractor shall provide computer security services to the U.S. Nuclear Regulatory Commission (NRC), to both the Office of Nuclear Security and Incident Response (NSIR) and to the Office of Chief Information Officer (OCIO), for the Division of Incident Response Operations systems: Operations Center Information Management System (OCIMS), Emergency Response Data System (ERDS) and the Emergency Telecommunications System (ETS).

The mission of the NRC is to ensure adequate protection for the public health and safety, promote the common defense and security, and protect the environment in regulating the Nation's civilian uses of nuclear fuels and material. In this undertaking, the NRC oversees nuclear power plants, non-power reactors, nuclear fuel cycle facilities, waste disposal, and the industrial and medical uses of nuclear materials. NRC works closely with its licensees and with local, State, other Federal and international organizations to achieve its goals in the event of an emergency.

In accordance with the Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources* and the Federal Information Security Management Act (FISMA), the NRC is required to perform risk assessments, develop system security plans, develop security test and evaluation plans, perform testing of security controls, develop information technology (IT) contingency plans, provide IT contingency plan training to personnel, develop test plans for IT contingency plans, perform testing of IT contingency plans, and develop a system certification report for its information resources.

The NRC requires the support of a Contractor to initially review all security and non security documentation for the OCIMS, ERDS, and ETS. Subsequently, the contractor, using the U. S. Department of Commerce Abbreviated Certification Methodology For Sensitive Information Technology Systems and guidance contained in NIST Special Pub. 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," NRC Management Directive 12.5, "NRC Automated Information Security Program," specifically Handbook 12.5, Part 4, "Certification and Accreditation," and other relevant NIST publications will perform a security re-certification and re-accreditation of each of these systems. This activity will include, but not be limited to (1) Examining the system's sensitivity and criticality to provide an assessment of its value to the organization, (2) Assessing the exposure of the system(s) and its associated assets (hardware, software, data) to both external and internal threats, (3) Assigning appropriate levels of concern (low, moderate, high) for both sensitivity/criticality and exposure, (4) Developing a Security Test and Evaluation (ST&E) Plan, (5) Exercising the ST&E Plan and preparing a ST&E Report, and (6) Preparing the Certification Report With Certification Signature.

The Contractor shall prepare the Re-certification / Re-accreditation Report. The system(s) Security Test & Evaluation (ST&E) Plan, security controls testing, and ST&E Report, which were completed between December 2000 and April 2001, are available electronically from the NRC Project Officer. It is envisioned that these documents will be modified to insure that they are in compliance with the latest security directives and policy.

1.1 SYSTEM DESCRIPTION

The NRC Operations Center (NRCOC) relies on the Emergency Telecommunication System (ETS) to ensure the timely flow of information during an emergency. ETS provides voice and data communications in the NRCOC. The NRCOC also relies on the Operations Center Information Management System (OCIMS) and the Emergency Response Data System (ERDS). OCIMS is the primary means of creating, storing, sending, and retrieving information in the NRCOC. The ERDS provides near real-time data from nuclear power plants during declared emergencies. These three (3) systems are described briefly below.

- OCIMS is the primary means of creating, storing, sending, and retrieving information in the NRCOC, and is referred to as the OCIMS local area network (LAN). The OCIMS network is a private data network configured in a star topology, providing networking services to its three (3) subsystems (data, display, and voice). During a response to an emergency, OCIMS supports NRC's vital role in providing leadership focus for national and international information distribution and decision support.

- ETS is the telecommunications network (telephone circuits and equipment) that NRC relies on during an emergency for voice and data communication between the NRCOC and the emergency response facilities (control room, technical support center, and emergency operations facility) associated with every commercial nuclear power plant and major fuel cycle facility. The ETS communication links to NRC licensed facilities are carried on dedicated lines to the Federal Telecommunications System (FTS) 2001 network. The FTS 2001 network is essentially separate from the public switched telephone network.

- ERDS is a real-time data system that allows safety-related information to be downloaded from nuclear power plant computers to the NRCOC. The ERDS collects plant performance and environmental data from 72 commercial nuclear power reactor sites regulated by the NRC. The transmission of data to ERDS is initiated at the reactor unit following the declaration of an alert or higher event classification. The standalone workstation at the reactor site dials-in to the NRC Headquarters (HQ) ERDS to allow the custom generation and display of trend plots and data. All dial-ins are validated under the VAX/VMS operating system security controls.

1.2 SYSTEMS ENVIRONMENT

1.2.1 OCIMS SYSTEM ARCHITECTURE

1.2.1.1 OCIMS Data Subsystem

The OCIMS Data Subsystem is comprised of the Response Computer System (RCS) and the

Headquarters Operations Officer (HOO) system. The RCS system is an application that provides a framework to support and facilitate the creation of documents and briefing materials used during incident response, and the HOO system is an application used by HOOs to manage information pertaining to the daily operational status of nuclear facilities and nuclear events. The RCS system comprises two (2) servers using Novell 4.11, one (1) server using Microsoft NT 4.0 and Citrix Metaframe 1.8, 50 workstations, 15 notebook computers, and eight (8) printers and seventeen (17) portable printers. The HOO system comprises three (3) servers using Windows NT 4.0, four (4) workstations, and four (4) printers. The OCIMS network includes a Nortel Baystack 450 Ethernet switch, providing a 10/100 Base-T Ethernet Link with connections to an Ethernet Router that provides access to the NRC wide area network (WAN) and e-mail system, and connections to a Cisco 2500 Router that provides access to the ERDS network.

1.2.1.2 OCIMS Network

The OCIMS network is a private data network that uses a star topology, providing network services to as many as 100 different accounts. The OCIMS network is 10/100 BaseT 802.3 Ethernet accommodating the Internetwork Packet Exchange/Serial Packet Exchange (IPX/SPX), Transmission Control Protocol/Internet Protocol (TCP/IP), and NetBIOS Extended User Interface (NetBEUI) protocols. All connections go through a Nortel Baystack 450 switch that has a maximum capacity of 96 ports. The Baystack switch is independent of the NRC's Agency network infrastructure. The OCIMS network's only external connection to NRC's Agency network infrastructure is to a single router. OCIMS users connect to that router whenever they have to access the Internet or NRC's e-mail system.

1.2.1.3 OCIMS Servers (RCS)

The Data Subsystem comprises two (2) Novell servers and a Microsoft NT 4.0 server. Each server supports various activities surrounding the RCS. Mainly, they provide users at NRC HQ and in the regions with network file and print services during drills and emergencies. They also provide an interface to the Display Subsystem.

The primary Novell server, OCIMS, is a Dell PowerEdge 2300 server providing NetWare 4.11 file/print services to NRC staff using the RCS system. There is also a backup Novell server available for use whenever the primary server experiences critical hardware or software failures. The backup server, OCIMSB, is also a Dell PowerEdge 2300 server capable of providing the same level of NetWare 4.11 file/print services to staff who use the RCS software. Both of these servers are connected to a Dell SDS-100 shareable disk cabinet. The Dell SDS-100 cabinet is currently configured with a 2x4 Small Computer System Interface (SCSI) backplane (two [2] server attachments and four [4] disks per server). The 2x4 SCSI backplane allows hot disk swapping, meaning, in the event of a primary server failure, an OCIMS System Administrator can relocate one or more disks, normally used on the primary server, to the backup server without having to shut off the power source to the Dell SDS-100 cabinet.

Each Dell server has a 350MHz main processor and is Pentium-based. Each is configured with 256MB of memory and two (2) 4.5GB internal disk drives. Each is equipped with two (2) Intel EtherExpress Pro 100 network interface cards, a Compact Disk-Read Only Memory (CD-ROM) drive, and one (1) internal Exabyte 8mm Tape drive. The Dell SDS-100 shareable disk cabinet holds two (2) 9GB external disk drives in the primary plane (used by the main server), and two (2) 18GB disk drives in the secondary plane (used by the secondary server). Each server's

operating system is DOS 6.22/NetWare 4.11 (100 user) with NetWare Support Pack 5b.

The third server, called OCIMSC, provides asynchronous communications service (ACS) to remote RCS users. The remote RCS users, after successfully attaching to the OCIMSC server, are routed to the primary RCS server, OCIMS, to access and use the RCS software. The OCIMSC server is a Dell PowerEdge 4400 that operates under Microsoft NT 4 with service pack 6a. It utilizes Citrix Metaframe 1.8 software to allow the remote RCS notebooks to dial-in. This server has a 866 MHz Pentium 4 processor, 256 MB of memory and two (2) 9 GB internal disk drives, it also has two (2) Intel EtherExpress 10/100 network cards.

Asynchronous Services are provided by a Comptrol Rocket Port card and twelve (12) 56 Kbps US Robotics external modems. Eight (8) of these modems are used for incoming phone lines to allow regional laptops to log-in to the server.

1.2.1.4 OCIMS Microsoft Windows NT Servers (HOO)

The Data Subsystem also comprises three (3) Microsoft Windows NT servers. Each server supports various activities surrounding the HOO. Mainly, they provide HOOs with network file and print services.

The primary Windows NT server, HOOSRVR1, is a Dell PowerEdge 2300 providing Windows NT Server 4.0 file/print services, and access to a SYBASE database for the NRC duty officers using the HOO system software. There is also a backup Windows NT server available for use whenever the primary server experiences critical hardware or software failures. The backup server, HOOSRVR2, is also a Dell PowerEdge 2300 server capable of providing the same level of file/print and database services to staff using the HOO system software.

Both servers have a 500MHz main processor and are Pentium-based. Each is configured with 512MB of memory and two (2) 9.1GB internal disk drives. Each is equipped with an Intel EtherExpress Pro 100 network interface card, a CD-ROM drive, and one (1) internal 12/24GB DAT 4mm tape drive. Each server's operating system is Microsoft Windows NT Server 4.0 with Service Pack 6a.

The third Windows NT server is located in the Region IV Incident Response Center. The server, called HOOREG04, is a Dell PowerEdge 2400. It has a 733MHz main processor and is Pentium-based. It is configured with 512MB of memory and two (2) 9GB internal disk drives. It also has an on-board Intel Pro 100+ network interface card, a CD-ROM drive, and one (1) internal Dell DDS4 power vault tape drive.

1.2.1.5 OCIMS Workstations

The workstations comprising the OCIMS network either support the HOO, RCS, or ERDS incident response systems. These PC's are Dell Precision 340 2.2 GHz computers with an 80GB hard drive. Most of the workstations have 512 MB of memory but ten (10) of them have 1 GB of memory. Most of the workstations operate with Windows NT 4.0 Workstation Service Pack 6a. The RCS workstations are being scheduled to be upgraded to Windows XP within the next six months.

1.2.1.6 OCIMS Display Subsystem

The OCIMS Display Subsystem provides the capability of displaying composite video and static images on display monitors in the NRCOC during incident response. The Display Subsystem comprises a Crestron Control System, an Autopatch Distribution Matrix, and primarily Mitsubishi 40 inch and Clarity 50 inch monitors. There is also a Cubix System consisting of four (4) Blade Enclosures with six (6) XP4 blades each for a total of twenty-four (24) blades. Each blade has a Xeon Pentium 4 processor with 512 MB of memory, a forty (40) GB internal drive, one (1) gigabit onboard Ethernet card and two (2) 10/100 onboard Ethernet cards. There is also one (1) Pentium-based, NEC workstation, referred to as the Display Control workstation, that interfaces with the Crestron Control System. It controls which set of 14 RCS static images are to be displayed (RCS practice, exercise, or events 1-4).

All twenty-four (24) of the blades use Windows XP. Fourteen (14) of these blades are used to supply static images to the Display subsystem. Nine (9) of them are used to support the Message Board displays. The last blade will be used to replace the Display system interface computer.

1.2.1.7 OCIMS Voice Subsystem

Within OCIMS, the Voice Subsystem provides the NRCOC with the ability to communicate externally. The Voice Subsystem includes the Executive Team (ET) teleconferencing system and interfaces to the NRCOC private branch exchange (PBX) and associated telephone equipment (such as the multichannel digital recorders). All voice communication into and out of the NRCOC is routed through the PBX. The PBX and its associated uninterruptible power supply (UPS), the Spectel Conference Bridge equipment, and the primary communications cable distribution point are all located in the telephone equipment room in the NRCOC. There is an Spectel Conference Bridge terminal at two (2) of the three (3) HOO stations in the NRCOC, at the remote HOO station in the Ready Room, and at the ET Secretaries position within the Executive Team Support Team area. The HOO staff uses these terminals to establish conference calls and to hold Commissioners Assistant briefings. It is also used to establish bridges, such as the Emergency Notification System (ENS) Bridge during incident response. A continuously operating multichannel recorder records all communications with the HOO, including calls transferred to the Spectel Conference Bridge. Phone communications throughout the NRCOC team areas are also recorded during events and exercises on the multichannel recorder. Three (3) fax machines are located in the Operational Support Team (OST) area and another three (3) fax machines are located in the HOO area. They are primarily used to send information to anyone that cannot be reached through e-mail and also provide a backup method of transmitting information if e-mail becomes unavailable. There are also STE phones with fax capability in the Safeguards Team (SGT) area and the HOO area. These are reserved for sensitive communications.

1.2.1.8 Executive Team Briefing System

The ET Briefing System provides ET members the ability to communicate, using the teleconferencing bridge system, with NRC regional management, the State Governor's office, the White House, and other high ranking government officials. There are three (3) AMX controllers in the ET area. These controllers give ET staff members the ability to connect or disconnect the ET bridge, control or mute call volume, enable audio in the ET room so that HQ staff can hear the communication, and establish and control a separate call for Base Team Managers. The

AMX interfaces these controls with a Gentner TI7200 and an IRP System 41. Additionally, the ET Briefing System is recorded for the duration of a briefing on the multichannel recorder.

1.2.2 ETS SYSTEM ARCHITECTURE

The Emergency Telecommunications System (ETS) currently provides reliable long distance telephone service to nuclear power plants and remote Emergency Operations Facilities for seven (7) essential NRC telecommunication functions. NRC uses the functions it provides during emergencies. Service is provided using direct access lines to the Federal Telecommunications System (FTS) network, which is currently supported by Worldcom.

1.2.3 ERDS SYSTEM ARCHITECTURE

The ERDS design concept embodies automatic acquisition of a predetermined list of nuclear power plant parameters, with electronic transmission of the data over standard telephone lines, to a computer at the NRCOC. On receipt, the data is automatically converted to a standard format for display, logging, and archival. The data is displayed on equipment installed at the NRCOC and Incident Response Centers in the Regional Offices. Access is also provided to other users, such as the affected state agencies and the NRC Technical Training Center (TTC).

The ERDS is designed to receive data from up to four (4) nuclear power plants and simultaneously process, display, and archive that data. Once the data is received, it is stored in a raw data file and then processed for display and future archival. A data viewer is used to view the received data in tabular and graphical form.

The ERDS hardware system is composed of three (3) main component subsystems: the Host Computer Subsystem, the Human-Computer Interface (HCI), and the Communication Subsystem. The Host Computer Subsystem consists of dual Compaq (formerly DEC) AlphaServer 1000 systems and their peripherals as well as a shared disk and shared tape drive housed in an R400X cabinet. The HCI consists of personal computer (PC) workstations, printers, and displays. The Communication Subsystem consists of a T-Bar communication switch, Codex modems, Motorola modems, Compaq DECServer 700s, and an Ethernet LAN.

In addition to several ERDS workstations located at the NRCOC, workstations are located at all four (4) NRC Regional Offices, as well as the TTC and several State Emergency Response Offices. The workstations at the NRCOC communicate with the host central processing unit (CPU) via the NRC wide area network (WAN). The workstations at the TTC and state offices communicate via the modem interface to the ERDS network segment. The workstations at the Regional Offices communicate primarily over the WAN but may also use modem interface.

All modems are connected through the DECServer 700s. The ports connected to the nuclear power plants access modems are configured as serial ports. The ports connected to the user modems are configured as point-to-point protocol (PPP) ports. In addition, there is one (1) modem and port configured for terminal dial-up access to the Alpha computers.

The modems are connected to the T-Bar and it is connected to the DECServer 700s. Switched connections through the T-Bar are controlled from the DEC AlphaServer 1000 hosts via RS-232 connections. The DECServer 700s are connected to the DEC AlphaServers via an Ethernet segment specific to ERDS. The ERDS subnet is separated from the OCIMS LAN Line (OCL)

via a router that is configured to maintain a firewall. The OCL is connected to the NRC WAN through the NRCHOC hub.

The ERDS host computers and all network devices on the ERDS subnet are connected to a SynOptics LattisHub 2813-05 16-port 10BaseT Ethernet Concentrator located in the NRCOC ERDS Computer Room. DEC 10BaseT cables are used as the interface from both Alpha 1000 systems to the hub. This concentrator box connects to each of the DECServer 700s to provide a communications path between the RS232 input from the modems to the AlphaServer 1000s. In addition, the concentrator provides a single connection to a Cisco router.

A Cisco Model 2514 router is installed between the NRCOC hub and the ERDS subnet hub. A twisted pair cable is pulled from the NRCOC to the ERDS Computer Room to connect the router to the NRCOC hub and 10Base2 is used to connect the Cisco router to the SynOptics LattisHub. The router is configured to act as a firewall between the ERDS subnet and the OCIMS LAN. The firewall prevents remote R*TIME/WIN Data Viewer users (or any dial-in connection through the ERDS modem pool) from accessing any resource on the OCIMS LAN, other than the ERDS-related data services, while still allowing the NRC Regional Offices to access the ERDS data services via the NRC WAN. In addition, the router isolates ERDS-related network traffic to the ERDS subnet.

The Alpha computers are running OpenVMS V.7.1 with DECNet for communications between the two (2) computers. A DECCluster has been configured with the two (2) Alpha computers and the shared disk drive. The TCP/IP services are provided by process Software's TCPWare. This software has been configured to only accept connections to the ERDS well-known port. In addition, the custom ERDS software is running on the computers. Upon startup, it allocates the ports the nuclear power plants connect through and then services all connection attempts through those ports. ERDS is running 100% of the time on both computers unless one (1) has been taken down for maintenance. OpenVMS security is used for the terminal access port.

ERDS users access ERDS through data viewer software, R*TIME/WIN, loaded on PCs running Windows NT and XP. Remote users dial-in to ERDS through modems and the TCP/IP networking software that comes with Windows (Dial-Up Networking). Once the modem connection is made, the users must log into the DECServer in order to complete the dial-up networking connection. At that point, the user must bring up the R*TIME/WIN software and log into it prior to being allowed access to the ERDS data.

In addition to the hardware described above, there is a ERDS backup system at Scientech's facility. It is very similar to the production ERDS computers but does not have the DECCluster with the shared disk and tape drives, has fewer modems and DECServers, and is not connected to the NRC WAN.

2.0 SCOPE OF WORK

2.1 Plans for Performance

NRC requires the Contractor to complete this project in four (4) milestones and corresponding deliverables on a firm fixed priced (FFP) basis. Each milestone consists of performing required tasks resulting in specific deliverables, as described below:

- Milestone 1: Develop a Security Test and Evaluation Plan
- Milestone 2: Conduct Security Test & Evaluation and Prepare Report
- Milestone 3: Prepare Re-certification/Re-Accreditation Report
- Milestone 4: Exit Briefing

The Contractor shall ensure that specifics pertaining to the system are fully addressed and that final deliverables can "stand-alone" serving as independent documents required for system certification.

2.2 TECHNICAL REQUIREMENTS

2.2.1 Milestone 1: Develop Security Test & Evaluation Plan

Having reviewed all available system and system security documentation, the Contractor shall develop an *Security Test & Evaluation (ST&E) Plan* for OCIMS, ERDS and ETS . The Contractor shall utilize the Department of Commerce (DOC) Abbreviated Certification Methodology Worksheets 1-4 to document the system description, identified vulnerabilities, security features, and security tests. (The DOC abbreviated certification methodology is available on the NIST Computer Security website, (http://csrc.ncsl.nist.gov/secpubs/)). Additionally, the Contractor shall conduct security testing for the management, operational, and technical security control measures and safeguards for OCIMS, ERDS and ETS. The Contractor shall utilize the DOC Abbreviated Certification Methodology Worksheet 5 to document the security test results. The recommendations for mitigating identified system risks shall be categorized according to low, medium, or high. The ST&E Plan will be approved by the NRC.

2.2.2 Milestone 2: Conduct ST&E and Prepare Report

The Contractor shall conduct the ST&E and then develop a *Security Test & Evaluation (ST&E) Report* for OCIMS, ERDS and ETS.

2.2.3 Milestone 3: Prepare Re-certification/Re-Accreditation Report

Finally, the Contractor shall then prepare the Re-certification/Re-accreditation Report for OCIMS, ERDS and ETS.

2.2.4 Milestone 4: Exit Briefing

The Contractor shall develop an *Exit Briefing* with NRC staff. The briefing shall include a brief summary of the work performed, provide the Re-certification/Re-accreditation Report and other documents prepared, and answer NRC staff questions.

2.3 Schedule of Deliverables

See SECTION B, subsection B.4TABLE OF DELIVERABLES AND SCHEDULE OF DELIVERY.

3.0 52.242-15 STOP WORK ORDER

(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 delivery order for a period of ninety (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 ninety (90) days after a stop-work order 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 delivery order.

(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 delivery order price, or both, and the delivery order 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 delivery order; 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 a proposal submitted at any time before final payment under this delivery order.

(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.

4.0 MEETINGS AND DELIVERABLES

KICK-OFF MEETING

The contractor shall attend a kick-off meeting within five (5) business days after task award to introduce the NRC Project Officer and the Technical Project Officer. During this meeting, discussion shall include the four (4) milestones and corresponding deliverables as identified in Section 2.0 - Scope of Work.

The Contractor shall deliver four (4) copies of all earlier specified deliverables to the NRC Project Officer during normal business hours. Final deliverables shall also be made electronically available in either MS Word or Corel WordPerfect 8 format on a 3.5 inch virus-free diskette or CD-ROM. The NRC shall have three (3) working days to review Draft deliverables and three (3) working days to review Final deliverables, and to accept or reject the

deliverable in writing.

In addition to the formal deliverables, the Contractor shall conduct, at a minimum, one (1) meeting every two (2) weeks between the Contractor and key client personnel. The meeting shall take place at the office of the Project Officer. Based on the clients work schedule, this meeting can be held by phone at the request of the client.

5.0 PERIOD OF PERFORMANCE

The period of performance for this delivery order is from July 27, 2004 through September 30, 2004.

6.0 TRAVEL

None

7.0 PROJECT OFFICER AUTHORITY (February 2004)

(a) The contracting officer's authorized representative hereinafter referred to as the project officer for this contract is:

Name: Mrs. Clarissa L. Evans Brown
Address: U. S. Nuclear Regulatory Commission
Office of Nuclear Security and Incident Response Operations
Mail Stop T-4L7
Washington, D. C. 20555-0001
Telephone Number: (301) 415-6891

(b) Performance of the work under this contract is subject to the technical direction of the NRC project officer. The term "technical direction" is defined to include the following:

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

(c) Technical direction must be within the general statement of work stated in the contract. The project officer does not have the authority to and may not issue any technical direction which:

(1) Constitutes an assignment of work outside the general scope of the contract.

(2) Constitutes a change as defined in the "Changes" clause of this contract.

(3) In any way causes an increase or decrease in the total estimated contract cost, the fixed fee, if any, or the time required for contract performance.

(4) Changes any of the expressed terms, conditions, or specifications of the contract.

(5) Terminates the contract, settles any claim or dispute arising under the contract, or issues any unilateral directive whatever.

(d) All technical directions must be issued in writing by the project officer or must be confirmed by the project officer in writing within ten (10) working days after verbal issuance. A copy of the written direction must be furnished to the contracting officer. A copy of NRC Form 445, Request for Approval of Official Foreign Travel, which has received final approval from the NRC must be furnished to the contracting officer.

(e) The contractor shall proceed promptly with the performance of technical directions duly issued by the project officer in the manner prescribed by this clause and within the project officer's authority under the provisions of this clause.

(f) If, in the opinion of the contractor, any instruction or direction issued by the project officer is within one of the categories as defined in paragraph (c) of this section, the contractor may not proceed but shall notify the contracting officer in writing within five (5) working days after the receipt of any instruction or direction and shall request the contracting officer to modify the contract accordingly. Upon receiving the notification from the contractor, the contracting officer shall issue an appropriate contract modification or advise the contractor in writing that, in the contracting officer's opinion, the technical direction is within the scope of this article and does not constitute a change under the "Changes" clause.

(g) Any unauthorized commitment or direction issued by the project officer may result in an unnecessary delay in the contractor's performance and may even result in the contractor expending funds for unallowable costs under the contract.

(h) A failure of the parties to agree upon the nature of the instruction or direction or upon the contract action to be taken with respect thereto is subject to 52.233-1 - Disputes.

(i) In addition to providing technical direction as defined in paragraph (b) of the section, the project officer shall:

(1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.

(2) Assist the contractor in the resolution of technical problems encountered during performance.

(3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination."

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(End of Clause)

8.0 GOVERNMENT-FURNISHED MATERIALS

The NRC Technical Project Officer will furnish to the contractor the following documents for use in the completion of tasks required by this SOW. Other relevant documents are available from the NIST web site at *http://csrc.nist.gov/publications/* :

- NRC Management Directive 12.5, NRC Automated Information Systems Security Program.
- NRC OCIO System Development and Life Cycle Management (SDLCM) Methodology, Version 1.2, January 31, 2001.(Latest Version)
- NIST Special Pub. 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"

9.0 2052.204-70 SECURITY (March 2004)

(a) Contract Security and/or Classification Requirements (NRC Form 187). The policies, procedures, and criteria of the NRC Security Program, NRC Management Directive (MD) 12 (including MD 12.1, "NRC Facility Security Program;" MD 12.2, "NRC Classified Information Security Program;" MD 12.3, "NRC Personnel Security Program;" MD 12.4, "NRC Telecommunications Systems Security Program;" MD 12.5, "NRC Automated Information Systems Security Program;" and MD 12.6, "NRC Sensitive Unclassified Information Security Program"), apply to performance of this contract, subcontract or other activity. This MD is incorporated into this contract by reference as though fully set forth herein. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified Restricted Data or National Security Information or matter, access to unclassified Safeguards Information, access to sensitive Information Technology (IT) systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants.

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract,

transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, safeguards information, proprietary data (trade secrets) or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, other (Official Use Only) internal data protected by the Privacy Act of 1974 (Pub. L. 93-579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor shall ensure that information protected from public disclosure is maintained as required by NRC regulations and policies, as cited in this contract or as otherwise provided by the NRC. The contractor will not directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security (DFS) and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

The contractor agrees to comply with the security requirements set forth in NRC Management Directive 12.1, NRC Facility Security Program which is incorporated into this contract by reference as though fully set forth herein. Attention is directed specifically to the section titled "Infractions and Violations," including "Administrative Actions" and "Reporting Infractions."

(e) Definition of National Security Information. The term National Security Information, as used in this clause, means information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and that is so designated.

(f) Definition of Restricted Data. The term Restricted Data, as used in this clause, means all data concerning design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but does not include data declassified or removed from the Restricted Data category pursuant to Section 142 of the Atomic Energy Act of 1954, as amended.

(g) Definition of Formerly Restricted Data. The term Formerly Restricted Data, as used in this clause, means all data removed from the Restricted Data category under Section 142-d of the Atomic Energy Act of 1954, as amended.

(h) Definition of Safeguards Information. Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production of utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

(i) Security Clearance. The contractor may not permit any individual to have access to Restricted Data, Formerly Restricted Data, or other classified information, except in accordance with the Atomic Energy Act of 1954, as amended, and the Commission's regulations or requirements applicable to the particular type or category of classified information to which access is required. The contractor shall also execute a Standard Form 312, Classified Information Nondisclosure Agreement, when access to classified information is required.

(j) Criminal Liabilities. It is understood that disclosure of National Security Information, Restricted Data, and Formerly Restricted Data relating to the work or services ordered hereunder to any person not entitled to receive it, or failure to safeguard any Restricted Data, Formerly Restricted Data, or any other classified matter that may come to the contractor or any person under the contractor's control in connection with work under this contract, may subject the contractor, its agents, employees, or subcontractors to criminal liability under the laws of the United States. (See the Atomic Energy Act of 1954, as amended, 42 U.S.C. 2011 et seq.; 18 U.S.C. 793 and 794; and Executive Order 12958.)

(k) Subcontracts and Purchase Orders. Except as otherwise authorized in writing by the contracting officer, the contractor shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(l) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

(End of Clause)

10.0 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS APPROVAL (February 2004)

The proposer/contractor must identify all individuals and propose the level of Information Technology (IT) approval for each, using the following guidance. The NRC sponsoring office shall make the final determination of the level, if any, of IT approval required for all individuals working under this contract.

The Government shall have and exercise full and complete control over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract.

SECURITY REQUIREMENTS FOR LEVEL I

Performance under this contract will involve prime contractor personnel, subcontractors or others who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I).

The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high

risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and will require a favorably adjudicated Limited Background Investigation (LBI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms and checks. Final access will be approved based on a favorably adjudicated LBI in accordance with the procedures found in NRC MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to SB/ DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3 which is incorporated into this contract by reference as though fully set forth herein. Based on SB review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E. O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

SECURITY REQUIREMENTS FOR LEVEL II

Performance under this contract will involve contractor personnel that develop and/or analyze sensitive information technology systems or data or otherwise have access to such systems or data (IT Level II).

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions. Such contractor personnel shall be subject to the NRC contractor personnel requirements of MD 12.3, Part I, which is hereby

incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Access National Agency Check with Inquiries (ANACI).

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by SB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final access will be approved based on a favorably adjudicated ANACI in accordance with the procedures found in MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC SB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E.O. 12968.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) which furnishes the basis for providing security requirements to prime contractors, subcontractors or others (e.g. bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of 30 days) to NRC Headquarters controlled buildings; or otherwise requires issuance of an NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for investigation is to be withdrawn or canceled, the contractor shall immediately notify the Project Officer by telephone in order that he/she will immediately contact the SB/DFS so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing to the Project Officer who will forward the confirmation via email to the SB/DFS. Additionally, SB/DFS must be immediately notified when an individual no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of an individual who has been

approved for or is being processed for access under the NRC "Personnel Security Program."

(End of Clause)

11.0 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY (IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002)

As part of contract performance the NRC may provide the contractor with information technology (IT) equipment and IT services or IT access as identified in the solicitation or subsequently as identified in the contract or delivery order. Government furnished IT equipment, or IT services, or IT access may include but is not limited to computers, copiers, facsimile machines, printers, pagers, software, phones, Internet access and use, and email access and use. The contractor (including the contractor's employees, consultants and subcontractors) shall use the government furnished IT equipment, and / or IT provided services, and/ or IT access solely to perform the necessary efforts required under the contract. The contractor (including the contractor's employees, consultants and subcontractors) are prohibited from engaging or using the government IT equipment and government provided IT services or IT access for any personal use, misuse, abuses or any other unauthorized usage.

The contractor is responsible for monitoring its employees, consultants and subcontractors to ensure that government furnished IT equipment and/ or IT services, and/ or IT access are not being used for personal use, misused or abused. The government reserves the right to withdraw or suspend the use of its government furnished IT equipment, IT services and/ or IT access arising from contractor personal usage, or misuse or abuse; and/ or to disallow any payments associated with contractor (including the contractor's employees, consultants and subcontractors) personal usage, misuses or abuses of IT equipment, IT services and/ or IT access; and/ or to terminate for cause the contract or delivery order arising from violation of this provision.)

ATTACHMENT A

Number	Title
1	NRC Form 187 - Contract Security and/or Classification Requirements
2	BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS

Attachment No. 1

NRC FORM 187
(1-2000)
NRCMD 12

U.S. NUCLEAR REGULATORY COMMISSION

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

AUTHORITY
The policies, procedures, and criteria of the NRC Security Program, NRCMD 12, apply to performance of this contract, subcontract or other activity.

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS

To be determined

A. CONTRACT NUMBER FOR COMMERCIAL CONTRACTS OR JOB CODE FOR DOE PROJECTS (Prime contract number must be shown for all subcontracts.)

B. PROJECTED START DATE	C. PROJECTED COMPLETION DATE
06/28/2004	09/30/2004

2. TYPE OF SUBMISSION

- [x] A. ORIGINAL
- [ ] B. REVISED (Supersedes all previous submissions)
- [ ] C. OTHER (Specify)

3. FOR FOLLOW-ON CONTRACT, ENTER PRECEDING CONTRACT NUMBER AND PROJECTED COMPLETION DATE

A. DOES NOT APPLY	B. CONTRACT NUMBER	DATE
[x]		

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

Computer Security Services for the NRC Division of Incident Response Operations, NSIR, systems: Operations Center Information Management System (OCIMS); Emergency Response Data System (ERDS); and Emergency Telecommunications System (ETS).

5. PERFORMANCE WILL REQUIRE

A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION

- [ ] YES (If "YES," answer 1-7 below)
- [x] NO (If "NO," proceed to 5.C.)

	NOT APPLICABLE	NATIONAL SECURITY		RESTRICTED DATA	
		SECRET	CONFIDENTIAL	SECRET	CONFIDENTIAL
1. ACCESS TO FOREIGN INTELLIGENCE INFORMATION	[ ]	[ ]	[ ]	[ ]	[ ]
2. RECEIPT, STORAGE, OR OTHER SAFEGUARDING OF CLASSIFIED MATTER. (See 5.B.)	[ ]	[ ]	[ ]	[ ]	[ ]
3. GENERATION OF CLASSIFIED MATTER.	[ ]	[ ]	[ ]	[ ]	[ ]
4. ACCESS TO CRYPTOGRAPHIC MATERIAL OR OTHER CLASSIFIED COMSEC INFORMATION.	[ ]	[ ]	[ ]	[ ]	[ ]
5. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION PROCESSED BY ANOTHER AGENCY.	[ ]	[ ]	[ ]	[ ]	[ ]
6. CLASSIFIED USE OF AN INFORMATION TECHNOLOGY PROCESSING SYSTEM.	[ ]	[ ]	[ ]	[ ]	[ ]
7. OTHER (Specify)	[ ]	[ ]	[ ]	[ ]	[ ]

B. IS FACILITY CLEARANCE REQUIRED? [ ] YES [x] NO

C. [ ] UNESCORTED ACCESS IS REQUIRED TO PROTECTED AND VITAL AREAS OF NUCLEAR POWER PLANTS.

D. [ ] ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION.

E. [x] ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.

F. [ ] UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.

FOR PROCEDURES AND REQUIREMENTS ON PROVIDING TEMPORARY AND FINAL APPROVAL FOR UNESCORTED ACCESS, REFER TO NRCMD 12.

*6. INFORMATION PERTAINING TO THESE REQUIREMENTS OR THIS PROJECT, EVEN THOUGH SUCH INFORMATION IS CONSIDERED UNCLASSIFIED, SHALL NOT BE RELEASED FOR DISSEMINATION EXCEPT AS APPROVED BY:

NAME AND TITLE	SIGNATURE	DATE
Richard H. Wessman, Director Incident Response Directorate Division of Preparedness and Response Office of Nuclear Security & Incident Response	R.H. Wessman	8/30/04

7. CLASSIFICATION GUIDANCE

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

8. CLASSIFIED REVIEW OF CONTRACTOR / SUBCONTRACTOR REPORT(S) AND OTHER DOCUMENTS WILL BE CONDUCTED BY:

- [ ] AUTHORIZED CLASSIFIER (Name and Title)
- [x] DIVISION OF FACILITIES AND SECURITY

9. REQUIRED DISTRIBUTION OF NRC FORM 187 *Check appropriate box(es)*

- [x] SPONSORING NRC OFFICE OR DIVISION (Item 10A)
- [x] DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT
- [x] DIVISION OF FACILITIES AND SECURITY (Item 10B)
- [x] CONTRACTOR (Item 1)
- [ ] SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

10. APPROVALS

SECURITY/CLASSIFICATION REQUIREMENTS FOR SUBCONTRACTS RESULTING FROM THIS CONTRACT WILL BE APPROVED BY THE OFFICIALS NAMED IN ITEMS 10B AND 10C BELOW.

NAME (Print or type)	SIGNATURE	DATE
A. DIRECTOR, OFFICE OR DIVISION Richard H. Wessman Director, Division of Incident Response Operations, NSIR	SIGNATURE R.H. Wessman	DATE 5/25/04
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY Thomas O. Martin, Director	SIGNATURE T.O. Martin	DATE 9/2/04
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements) Kathryn Greene, Director	SIGNATURE	DATE

REMARKS

Attachment No. 2

BILLING INSTRUCTIONS FOR
FIXED PRICE CONTRACTS (October 2003)(With Reimbursable Travel)

General: The contractor is responsible during performance and through final payment of this contract for the accuracy and completeness of the data within the Central Contractor Registration (CCR) database, and for any liability resulting from the Government's reliance on inaccurate or incomplete CCR data. **The contractor shall prepare vouchers or invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICES AS IMPROPER.**

Form: Claims shall be submitted on the payee's letterhead, voucher/invoices, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal--Continuation Sheet." These forms are available from the U.S. Government Printing Office, 710 North Capitol Street, Washington, DC 20401.

Number of Copies: An original and three copies shall be submitted. Failure to submit all the required copies will result in rejection of the voucher/invoice as improper.

Designated Agency Billing Office: Vouchers/Invoices shall be submitted to the following address:

U.S. Nuclear Regulatory Commission
Division of Contracts - T-7-I-2
Washington, DC 20555-0001

A copy of any invoice which includes a purchase of property valued at the time of purchase at $5000 or more, shall additionally be sent to:

NRC Property Management Officer
Administrative Services Center
Mail Stop -O-2G-112
Washington, DC 20555-0001

HAND-DELIVERY OF VOUCHERS/INVOICES IS DISCOURAGED AND WILL NOT EXPEDITE PROCESSING BY THE NRC. However, should you choose to deliver vouchers/invoices by hand, including delivery by any express mail service or special delivery service which uses a courier or other person to deliver the vouchers/invoices in person to the NRC, such vouchers/invoices must be addressed to the above Designated Agency Billing Office and will only be accepted at the following location:

U.S. Nuclear Regulatory Commission
One White Flint North - Mail Room
11555 Rockville Pike
Rockville, MD 20852

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED AT OTHER THAN THE ABOVE ADDRESS

Note that the official receipt date for hand-delivered vouchers/invoices will be the date it is received by the official agency billing office in the Division of Contracts.

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of the Standard Form 26 or Block 25 of the Standard Form 33, whichever is applicable.

Frequency: The contractor shall submit a voucher or invoice only after the NRC's final acceptance of services rendered or products delivered in performance of the contract unless otherwise specified in the contract.

Preparation and Itemization of the Voucher/Invoice: The voucher/invoice shall be prepared in ink or by typewriter (without strike-overs). Corrections or erasures must be initialed. To be considered a proper voucher/invoice, all of the following elements must be included:

1. Contractor's Data Universal Number (DUNS) or DUNS+4 number that identifies the contractor's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the contractor to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.

2. Contract number.

3. Sequential voucher/invoice number.

4. Date of voucher/invoice.

5. Payee's name and address. Show the name of the Payee as it appears in the contract and its correct address. If the Payee assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the Central Contractor Registration (CCR) database at http://www.ccr.gov and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).

6. Description of articles or services, quantity, unit price, and total amount.

7. For contractor acquired property list each item purchased costing $50,000 or more and having a life expectancy of more than 1 year and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.

8. Weight and zone of shipment, if shipped by parcel post.

9. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.

10. Instructions to consignee to notify the Contracting Officer of receipt of shipment.

11. For Indefinite Delivery contracts or contracts under which progress payments are authorized, the final voucher/invoice shall be marked "FINAL VOUCHER" OR "FINAL INVOICE."

Currency: Billings may be expressed in the currency normally used by the contractor in maintaining his accounting records and payments will be made in that currency. However, the U.S. dollar equivalent for all vouchers/invoices paid under the contract may not exceed the total U.S. dollars authorized in the contract.

Supersession: These instructions supersede any previous billing instructions.

C:\Documents and Settings\dak1.NRCDOMAIN\Desktop\CISSCO SECURITY PROCUREMENTS\SECURITY PROCUREMENT\NRC-03-04-029 COMPUTER SECURITY REV -UPDATE OF THE NRR RPS SYSTEM\Billing instruct FP 2003.wpd