Group A

FOIA/PA NO: 2015-0459

RECORDS BEING RELEASED IN THEIR ENTIRETY

2/18/2011 NRC Contract NRC-33-11-325 (292 pages)

Base Award

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
NRC-33-11-325				

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Pulaski, 301-492-3647
Mail Stop: TWB-01-B10M
Washington DC 20555 DC 20555

10. THIS ACQUISITION IS

[X] UNRESTRICTED OR [ ] SET ASIDE: % FOR:
[ ] SMALL BUSINESS
[ ] HUBZONE SMALL BUSINESS
[ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS [ ] 8(A)

NAICS: 541513
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
[X] SEE SCHEDULE	N/A	[ ]	N/A	[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO CODE

U.S. Nuclear Regulatory Commission
11545 Rockville Pike
Attn: Eric Brusoe
Mail Stop: T5-F27
Washington DC 20555 DC 20555

16. ADMINISTERED BY CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington DC 20555 DC 20555

17a. CONTRACTOR/OFFEROR CODE FACILITY CODE

PEROT SYSTEMS GOVERNMENT SERVICES, INC.

8270 WILLOW OAKS CORPORATE DR STE 300

FAIRFAX VA 220314514

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE 3100

Department of Interior / NBC
NRCPayments@nbc.gov
Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue
Denver CO 80235-2230

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
[ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with Information Technology Infrastructure Services and Support (ITISS) as described in Attachment A, Attachment D and in accordance with the terms and conditions of this contract and related orders.				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA
N/A.

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED.

[X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

[X] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)
Kathleen Hines	

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
KATHLEEN HINES	2-18-11	Jordan Pulaski Contracting Officer	2-18-11

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

DIRECTOR OF CONTRACTS

STANDARD FORM 1449 (REV. 10/2010)
Prescribed by GSA - FAR (48 CFR) 53.212

A-26

Table of Contents

PART I - THE SCHEDULE **B-4**

SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS **B-4**

B.1 ALLOWABLE CONTRACT TYPES FOR EACH SOW SECTION B-4
B.2 PROJECT TITLE B-5
B.3 BRIEF DESCRIPTION OF WORK (MAR 1987) B-5
B.4 CONTRACT TYPE B-5
B.5 CONTRACT CONSIDERATION AND MAXIMUM CONTRACT VALUE B-5

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK **C-1**

SECTION D - PACKAGING AND MARKING **D-1**

D.1 PACKAGING AND MARKING (MAR 1987) D-1

SECTION E - INSPECTION AND ACCEPTANCE **E-1**

E.1 PLACE OF INSPECTION AND ACCEPTANCE E-1

SECTION F - DELIVERIES OR PERFORMANCE **F-1**

F.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE F-1
F.2 2052.211-70 PREPARATION OF TECHNICAL REPORTS (JAN 1993) F-1
F.3 2052.211-71 TECHNICAL PROGRESS REPORT (JAN 1993) F-1
F.4 DELIVERY SCHEDULE F-1
F.5 PLACE OF DELIVERY--REPORTS (JUN 1988) F-2
F.7 DURATION OF CONTRACT PERIOD (MAR 1987) ALTERNATE 2 (MAR 1987) F-2

SECTION G - CONTRACT ADMINISTRATION DATA **G-1**

G.1 2052.215-71 PROJECT OFFICER AUTHORITY (NOVEMBER 2006) G-1

SECTION H - SPECIAL CONTRACT REQUIREMENTS **H-1**

H.1 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (JUN 2010) H-1
H.2 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) ALTERNATE I (OCT 2008) H-6
H.3 ADDENDUM to FAR 52.212-4 Contract Terms and Conditions-- Commercial Items H-15
H.4 2052.215-77 TRAVEL APPROVALS AND REIMBURSEMENT (Oct 1999) H-15
H.5 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006) H-16
H.6 2052.215-70 KEY PERSONNEL (JAN 1993) H-16
Core Services (PSOW Section C.5) H-16
Additional Services (PSOW Sections C.6.1, C.6.2, C.6.3, C.6.5, C.6.8, C.6.9) H-16
H.7 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL H-17
H.8 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (JUL 2007) H-17
H.9 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (JUL 2007) H-19
H.10 SEAT BELTS H-21
H.11 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY (IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002) H-21
H.12 COMPLIANCE WITH US IMMIGRATION LAWS AND REGULATIONS H-21
H.13 SAFETY ON-SITE CONTRACTOR PERSONNEL H-22
H.14 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2003) H-22

H.15 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (JULY 2006) H-22
H.16 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OVER CONTRACTOR H-23
H.17 2052.204.70 SECURITY (MAR 2004) H-24
H.18 PROJECT SUPPORT CONTRACTORS H-26
H.19 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE H-26
H.20 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (APRIL 2010) H-26
H.21 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) H-31
H.22 2052.209-72 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST (JAN 1993) H-31
H.23 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION OR PERFORMING IN ESPECIALLY SENSITIVE POSITIONS H-33
H.24 52.216-18 ORDERING (OCT 1995) H-34
H.25 52.216-19 ORDER LIMITATIONS (OCT 1995) H-34
H.26 52.216-22 INDEFINITE QUANTITY (OCT 1995) H-35
H.27 52.237-3 CONTINUITY OF SERVICES (JAN 1991) H-35

PART II - CONTRACT CLAUSES I-1

SECTION I - CONTRACT CLAUSES I-1

I.1 NOTICE OF ALLOWABLE CONTRACT TYPES I-1
I.2 52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (DEC 2007) I-1
I.3 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984) I-1

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS J-1

SECTION J - LIST OF ATTACHMENTS J-1

A STATEMENT OF WORK/SPECIFICATION J-1
B BILLING INSTRUCTIONS LABOR HOUR J-1
C BILLING INSTRUCTIONS FIXED PRICE J-1
D PRICE SCHEDULE J-1
E NRC 187 ..... J-1
F OCOI Guidelines J-1
G NRC-Approved Small Business Subcontracting Plan J-1

PART I - THE SCHEDULE

SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS

B.1 ALLOWABLE CONTRACT TYPES FOR EACH SOW SECTION

The contract types in this IDIQ contract are shown below.

Clauses designated with "$" to the left of the citation number are applicable to FIRM-FIXED-PRICE line items only.

Clauses designated with "&" to the left of the citation number are applicable to LABOR-HOUR line items only.

SOW Reference	Category/Item	Contract Type
C.5.1	Basic Infrastructure Support Services	
C.5.1.1	BlackBerry	firm-fixed-price
C.5.1.2	Electronic Mail (Email) and Messaging	firm–fixed-price
C.5.1.3	File and Print	firm-fixed-price
C.5.1.4	Personal Computing and Related Software Licensing	firm-fixed-price
C.5.1.5	Network Components	firm-fixed-price
C.5.1.6	Remote Access	firm-fixed-price
C.5.1.7	Integration	labor-hour
C.5.1.8	High Performance Computing	labor-hour
C.5.2	Service Delivery and Management Responsibilities	firm-fixed-price
C.6.1	Computer Facilities Management	firm-fixed-price
C.6.2	Operations Center Network Management	firm-fixed-price
C.6.3	Data Center System Administration	firm-fixed-price
C.6.4	Wireless Communications Services	
C.6.4.1	Telecommunications Management and Oversight	firm-fixed-price
C.6.4.2	Project Status Reports	firm-fixed-price
C.6.4.3	Telecommunications Support Services	
C.6.4.3.1	Maintenance of Property Management Records	firm-fixed-price
C.6.4.3.2	Wireless Hardware and services	firm-fixed-price
C.6.4.3.3	Products and Services	firm-fixed-price
C.6.4.4	Telecommunications Expense Management Services	firm-fixed-price
C.6.5	Software License Management	
C.6.5.1	Software Inventory	labor-hour
C.6.5.2	Planning and Design	labor-hour
C.6.5.3	Software License Management Tool	firm-fixed-price
C.6.5.4	Enterprise License Vendor Management	firm-fixed-price
C.6.5.5	Software Catalog	firm-fixed-price
C.6.5.6	Usage Reporting and Auditing	firm-fixed-price
C.6.6	Safeguards Local Area Network and Electronic Safe Services	firm-fixed-price
C.6.7	Technology Assessment Center	labor-hour
C.6.8	ERDS Operations and Maintenance	labor-hour/firm-fixed-price
C.6.9	Secure LAN and Electronic Safe	firm-fixed price
C.6.10	Development Facility	labor-hour/firm-fixed-price
C.6.11	Microsoft SharePoint Support	labor-hour
C.6.12	Extraordinary Move Support	firm-fixed-price
C.7	Transition	labor-hour/firm-fixed-price

B.2 PROJECT TITLE

The title of this project is as follows:

Information Technology Infrastructure Services and Support (ITISS).

B.3 BRIEF DESCRIPTION OF WORK (MAR 1987)

The purpose of this procurement is to acquire the technical services of an information technology (IT) provider to continue the support of the NRC IT Infrastructure (ITI). This new ITISS contract will continue to provide NRC Headquarters, Regional Offices, Resident Inspector Sites, the TTC, the High Level Waste Management Office, and mobile NRC users virtually anywhere in the world with the vast majority of needed IT services, including: desktop and laptop computers, servers, office productivity software, e-mail, help desk, BlackBerry devices, network file storage, network printers, network management, IT operational security, data back-up and recovery, and new technology integration.

B.4 CONTRACT TYPE

This is an indefinite delivery, indefinite quantity contract, containing firm-fixed-price and labor-hour line items.

B.5 CONTRACT CONSIDERATION AND MAXIMUM CONTRACT VALUE

The Government is obligated to order a minimum of $5,000,000.00 worth of services during the first 12 months of the base period of this contract. The maximum contract value is $270,000,000.00 should all three option periods be exercised. As option years are exercised, the total estimated amount for the option year being exercised will be added to the current contract value to calculate a new contract value as of that option year. The government may order up to the maximum value/quantity over the course of the entire six year period of this contract.

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 STATEMENT OF WORK

See Attachment A.

SECTION D - PACKAGING AND MARKING

D.1 PACKAGING AND MARKING (MAR 1987)

The Contractor shall package material for shipment to the NRC in such a manner that will ensure acceptance by common carrier and safe delivery at destination. Containers and closures shall comply with the Interstate Commerce Commission Regulations, Uniform Freight Classification Rules, or regulations of other carriers as applicable to the mode of transportation. On the front of the package, the Contractor shall clearly identify the contract number under which the product is being provided.

SECTION E - INSPECTION AND ACCEPTANCE

See clauses 52.212-4 and 52.212-4 Alternate I.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of the deliverable items to be furnished hereunder shall be made as specified in each order issued under this contract.

SECTION F - DELIVERIES OR PERFORMANCE

F.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract. See www.acquisition.gov/far for electronic access to the full text of a clause.

NUMBER	TITLE	DATE
	FEDERAL ACQUISITION REGULATION (48 CFR Chapter 1)	
52.242-15	STOP-WORK ORDER	AUG 1989
52.247-34	F.O.B. DESTINATION	NOV 1991
52.247-48	F.O.B. DESTINATION--EVIDENCE OF SHIPMENT	FEB 1999

F.2 2052.211-70 PREPARATION OF TECHNICAL REPORTS (JAN 1993)

All technical reports required by Section C and all Technical Progress Reports required by Section F are to be prepared in accordance with the attached Management Directive 3.8, "Unclassified Contractor and Grantee Publications in the NUREG Series." Management Directive 3.8 is not applicable to any Contractor Spending Plan (CSP) and any Financial Status Report that may be included in this contract. (See List of Attachments).

F.3 2052.211-71 TECHNICAL PROGRESS REPORT (JAN 1993)

The contractor shall provide a monthly Technical Progress Report to the project officer and the contracting officer. The report is due within 15 calendar days after the end of the report period and must identify the title of the project, the contract number, appropriate financial tracking code specified by the NRC Project Officer, project manager and/or principal investigator, the contract period of performance, and the period covered by the report. Each report must include the following for each discrete task/task order:

(a) A listing of the efforts completed during the period, and milestones reached or, if missed, an explanation provided;

(b) Any problems or delays encountered or anticipated and recommendations for resolution. If the recommended resolution involves a contract modification, e.g., change in work requirements, level of effort (cost) or schedule delay, the contractor shall submit a separate letter to the contracting officer identifying the required change and estimated cost impact.

(c) A summary of progress to date; and

(d) Plans for the next reporting period.

F.4 DELIVERY SCHEDULE

The delivery schedule will be specified in each order issued under this contract.

F.5 PLACE OF DELIVERY--REPORTS (JUN 1988)

The items to be furnished hereunder shall be delivered, with all charges paid by the Contractor, to:

(a) Project Officer (1 copy – via email)

See name and address in Section G.1

(b) Contracting Officer (1 copy – via email)

Jordan Pulaski

Email to: Jordan.Pulaski@nrc.gov

F.7 DURATION OF CONTRACT PERIOD (MAR 1987) ALTERNATE 2 (MAR 1987)

This contract shall commence on award date and will expire at the end of the Base Period. The term of this contract may be extended at the option of the Government in accordance with FAR clause 52.217-9, as follows:

Option Period 1 – one year, beginning the day after expiration of the Base Period
Option Period 2 – one year, beginning the day after expiration of Option Period 1
Option Period 3 – one year, beginning the day after expiration of Option Period 2

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 2052.215-71 PROJECT OFFICER AUTHORITY (NOVEMBER 2006)

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

PRIMARY

Name: Eric Brusoe

Address: U.S. Nuclear Regulatory Commission
Office of Information Services
11555 Rockville Pike, M/S T-5D14
Rockville, MD 20852

Telephone Number: 301-415-5053
Email Address: Eric.Brusoe@nrc.gov

ALTERNATE

Name: David Curtis

Address: U.S. Nuclear Regulatory Commission
Office of Information Services
11555 Rockville Pike, M/S T-5D14
Rockville, MD 20852

Telephone Number: 301-415-6012
Email Address: David.Curtis@nrc.gov

(b) Performance of the work under this contract is subject to the technical direction of the NRC Project Officer identified above or, in their absence, their alternate designated above. 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.

(7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the Contractor as part of closeout procedures, written certification that the Contractor has returned to NRC, transferred to the successor Contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (JUN 2010)

(a) *Inspection/Acceptance.* The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights --

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C.3727). However, when a third party makes payment (*e.g.,* use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes.* Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes.* This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions.* The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays.* The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.*

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include --

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payment.

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) Prompt Payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR Part 1315.

(3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount*. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments*. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall—

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—

(A) Circumstances of the overpayment (*e.g.*, duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected contract line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) Interest.

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in Section 611 of the Contract Disputes Act of 1978 (Public Law 95-563), which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period at fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final decisions. The Contracting Officer will issue a final decision as required by 33.211 if—

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss.* Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes.* The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience.* The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title.* Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty.* The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability.* Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances.* The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, *et seq.*, Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) *Order of precedence.* Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

(9) The specification.

(t) Central Contractor Registration (CCR).

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)

(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in Subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to:

(A) Change the name in the CCR database;

(B) Comply with the requirements of Subpart 42.12 of the FAR;

(C) Agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see FAR Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via the Internet at http://www.ccr.gov or by calling 1-888-227-2423, or 269-961-5757.

H.2 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (MAR 2009) ALTERNATE I (OCT 2008)

(Applies to all Labor-Hour CLINs in Section B.1.)

(a) Inspection/Acceptance.

(1) The Government has the right to inspect and test all materials furnished and services performed under this contract, to the extent practicable at all places and times, including the period of performance, and in any event before acceptance. The Government may also inspect the plant or plants of the Contractor or any subcontractor engaged in contract performance. The Government will perform inspections and tests in a manner that will not unduly delay the work.

(2) If the Government performs inspection or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish and shall require subcontractors to furnish all reasonable facilities and assistance for the safe and convenient performance of these duties.

(3) Unless otherwise specified in the contract, the Government will accept or reject services and materials at the place of delivery as promptly as practicable after delivery, and they will be presumed accepted 60 days after the date of delivery, unless accepted earlier.

(4) At any time during contract performance, but not later than 6 months (or such other time as may be specified in the contract) after acceptance of the services or materials last delivered under this contract, the Government may require the Contractor to replace or correct services or materials that at time of delivery failed to meet contract requirements. Except as otherwise specified in paragraph (a)(6) of this clause, the cost of replacement or correction shall be determined under paragraph (i) of this clause, but the "hourly rate" for labor hours incurred in the replacement or correction shall be reduced to exclude that portion of the rate attributable to profit. Unless otherwise specified below, the portion of the "hourly rate" attributable to profit shall be 10 percent. The Contractor shall not tender for acceptance materials and services required to be replaced or corrected without disclosing the former requirement for replacement or correction, and, when required, shall disclose the corrective action taken. [Insert portion of labor rate attributable to profit.]

(5)(i) If the Contractor fails to proceed with reasonable promptness to perform required replacement or correction, and if the replacement or correction can be performed within the ceiling price (or the ceiling price as increased by the Government), the Government may--

(A) By contract or otherwise, perform the replacement or correction, charge to the Contractor any increased cost, or deduct such increased cost from any amounts paid or due under this contract; or

(B) Terminate this contract for cause.

(ii) Failure to agree to the amount of increased cost to be charged to the Contractor shall be a dispute under the Disputes clause of the contract.

(6) Notwithstanding paragraphs (a)(4) and (5) above, the Government may at any time require the Contractor to remedy by correction or replacement, without cost to the Government, any failure by the Contractor to comply with the requirements of this contract, if the failure is due to--

(i) Fraud, lack of good faith, or willful misconduct on the part of the Contractor's managerial personnel; or

(ii) The conduct of one or more of the Contractor's employees selected or retained by the Contractor after any of the Contractor's managerial personnel has reasonable grounds to believe that the employee is habitually careless or unqualified.

(7) This clause applies in the same manner and to the same extent to corrected or replacement materials or services as to materials and services originally delivered under this contract.

(8) The Contractor has no obligation or liability under this contract to correct or replace materials and services that at time of delivery do not meet contract requirements, except as provided in this clause or as may be otherwise specified in the contract.

(9) Unless otherwise specified in the contract, the Contractor's obligation to correct or replace Government-furnished property shall be governed by the clause pertaining to Government property.

(b) Assignment. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Government wide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) Changes. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) Disputes. This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) Definitions.

(1) The clause at FAR 52.202-1, Definitions, is incorporated herein by reference. As used in this clause--

(i) Direct materials means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) Hourly rate means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are--

(A) Performed by the Contractor;

(B) Performed by the subcontractors; or

(C) Transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control.

(iii) Materials means--

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (e.g., incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.);

(D) The following subcontracts for services which are specifically excluded from the hourly rate: [Insert any subcontracts for services to be excluded from the hourly rates prescribed in the schedule.]; and

(E) Indirect costs specifically provided for in this clause.

(iv) Subcontract means any contract, as defined in FAR Subpart 2.1, entered into with a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract including transfers between divisions, subsidiaries, or affiliates of a Contractor or subcontractor. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(f) Excusable delays. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer-- Central Contractor Registration, or

52.232-34, Payment by Electronic Funds Transfer--Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) Patent indemnity. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payments.

(1) Services accepted. Payment shall be made for services accepted by the Government that have been delivered to the delivery destination(s) set forth in this contract. The Government will pay the Contractor as follows upon the submission of commercial invoices approved by the Contracting Officer:

(i) Hourly rate.

(A) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the contract by the number of direct labor hours performed. Fractional parts of an hour shall be payable on a prorated basis.

(B) The rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by individuals that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(C) Invoices may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer) to the Contracting Officer or the authorized representative.

(D) When requested by the Contracting Officer or the authorized representative, the Contractor shall substantiate invoices (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment, individual daily job timecards, records that verify the employees meet the qualifications for the labor categories specified in the contract, or other substantiation specified in the contract.

(E) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis.

(1) If no overtime rates are provided in the Schedule and the Contracting Officer approves overtime work in advance, overtime rates shall be negotiated.

(2) Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract.

(3) If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(ii) Materials.

(A) If the Contractor furnishes materials that meet the definition of a commercial item at FAR 2.101, the price to be paid for such materials shall be the Contractor's established catalog or market price, adjusted to reflect the--

(1) Quantities being acquired; and

(2) Any modifications necessary because of contract requirements.

(B) Except as provided for in paragraph (i)(1)(ii)(A) and (D)(2) of this clause, the Government will reimburse the Contractor the actual cost of materials (less any rebates, refunds, or discounts received by the Contractor that are identifiable to the contract) provided the Contractor--

(1) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or

(2) Makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.

(C) To the extent able, the Contractor shall--

(1) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and

(2) Give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that are identifiable to the contract.

(D) Other Costs. Unless listed below, other direct and indirect costs will not be reimbursed.

(1) Other Direct Costs. The Government will reimburse the Contractor on the basis of actual cost for the following, provided such costs comply with the requirements in paragraph (i)(1)(ii)(B) of this clause: [Insert each element of other direct costs (e.g., travel, computer usage charges, etc. Insert "None" if no reimbursement for other direct costs will be provided. If this is an indefinite delivery contract, the Contracting Officer may insert "Each order must list separately the elements of other direct charge(s) for that order or, if no reimbursement for other direct costs will be provided, insert 'None'."]

(2) Indirect Costs (Material Handling, Subcontract Administration, etc.). The Government will reimburse the Contractor for indirect costs on a pro-rata basis over the period of contract performance at the following fixed price: [Insert a fixed amount for the indirect costs and payment schedule. Insert "$0" if no fixed price reimbursement for indirect costs will be provided. (If this is an indefinite delivery contract, the Contracting Officer may insert "Each order must list separately the fixed amount for the indirect costs and payment schedule or, if no reimbursement for indirect costs, insert 'None')."]

(2) Total cost. It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during the performance of this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performance of this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(3) Ceiling price. The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(4) Access to records. At any time before final payment under this contract, the Contracting Officer (or authorized representative) will have access to the following (access shall be limited to the listing below unless otherwise agreed to by the Contractor and the Contracting Officer):

(i) Records that verify that the employees whose time has been included in any invoice meet the qualifications for the labor categories specified in the contract;

(ii) For labor hours (including any subcontractor hours reimbursed at the hourly rate in the schedule), when timecards are required as substantiation for payment--

(A) The original timecards (paper-based or electronic);

(B) The Contractor's timekeeping procedures;

(C) Contractor records that show the distribution of labor between jobs or contracts; and

(D) Employees whose time has been included in any invoice for the purpose of verifying that these employees have worked the hours shown on the invoices.

(iii) For material and subcontract costs that are reimbursed on the basis of actual cost--

(A) Any invoices or subcontract agreements substantiating material costs; and

(B) Any documents supporting payment of those invoices.

(5) Overpayments/Underpayments. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding invoices, that are found by the Contracting Officer not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. The Contractor shall promptly pay any such reduction within 30 days unless the parties agree otherwise. The Government within 30 days will pay any such increases, unless the parties agree otherwise. The Contractor's payment will be made by check. If the Contractor becomes aware of a duplicate invoice payment or that the Government has otherwise overpaid on an invoice payment, the Contractor shall--

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the--

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected contract line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6)(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury, as provided in Section 611 of the Contract Disputes Act of 1978 (Public Law 95-563), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six month period as established by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final Decisions. The Contracting Officer will issue a final decision as required by 33.211 if--

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt in a timely manner;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see FAR 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on--

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(viii) Upon receipt and approval of the invoice designated by the Contractor as the "completion invoice" and supporting documentation, and upon compliance by the Contractor with all terms of this contract, any outstanding balances will be paid within 30 days unless the parties agree otherwise. The completion invoice, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(7) Release of claims. The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions.

(i) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible to exact statement by the Contractor.

(ii) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(iii) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(8) Prompt payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(9) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(10) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(j) Risk of loss. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) Taxes. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) Termination for the Government's convenience. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid an amount for direct labor hours (as defined in the Schedule of the contract) determined by multiplying the number of direct labor hours expended before the effective date of termination by the hourly rate(s) in the contract, less any hourly rate payments already made to the Contractor plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system that have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

(m) Termination for cause. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to

provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government will not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) Title. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) Warranty. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) Limitation of liability. Except as otherwise provided by an express warranty, the Contractor shall not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) Other compliances. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, et seq., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; Section 1553 of the American Recovery and Reinvestment Act of 2009 relating to whistleblower protections for contracts funded under that Act; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) Order of precedence. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments

(9) The specification.

(t) Central Contractor Registration (CCR).

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate

and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in FAR subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the CCR database; (B) comply with the requirements of subpart 42.12; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor shall be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via the internet at http://www.ccr.gov or by calling 1-888-227-2423 or 269-961-5757.

H.3 ADDENDUM to FAR 52.212-4 Contract Terms and Conditions-- Commercial Items

Clauses that are incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The following clauses are incorporated as an addendum to this contract:

H.4 2052.215-77 TRAVEL APPROVALS AND REIMBURSEMENT (Oct 1999)

(a) All foreign travel must be approved in advance by the NRC on NRC Form 445, Request for Approval of Official Foreign Travel, and must be in compliance with FAR 52.247-63 Preference for U.S. Flag Air Carriers. The contractor shall submit NRC Form 445 to the NRC no later than 30 days before beginning travel.

(b) The contractor must receive written approval from the NRC Project Officer before taking travel that was unanticipated in the Schedule (i.e., travel not contemplated in the Statement of Work, or changes to specific travel identified in the Statement of Work).

(c) The contractor will be reimbursed only for travel costs incurred that are directly related to this contract and are allowable subject to the limitations prescribed in FAR 31.205-46.

(d) It is the responsibility of the contractor to notify the contracting officer in accordance with the Limitations of Cost clause of this contract when, at any time, the contractor learns that travel expenses will cause the contractor to exceed the estimated costs specified in the Schedule.

(e) Reasonable travel costs for research and related activities performed at State and nonprofit institutions, in accordance with Section 12 of Pub. L. 100-679, must be charged in accordance with the contractor's institutional policy to the degree that the limitations of Office of Management and Budget (OMB) guidance are not exceeded. Applicable guidance documents include OMB Circular A-87, Cost Principles for State and Local Governments; OMB

Circular A-122, Cost Principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.

H.5 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006)

During the life of this contract, the rights of ingress and egress for Contractor personnel must be made available, as required, provided that the individual has been approved for unescorted access after a favorable adjudication from the Security Branch, Division of Facilities and Security (SB/DFS).

In this regard, all Contractor personnel whose duties under this contract require their presence on site shall be clearly identifiable by a distinctive badge furnished by the NRC. The Project Officer shall assist the Contractor in obtaining badges for the Contractor personnel. All Contractor personnel must present two forms of Identity Source Documents (I-9). One of the documents must be a valid picture ID issued by a state or by the Federal Government. Original I-9 documents must be presented in person for certification. A list of acceptable documents can be found at http://www.usdoj.gov/crt/recruit_employ/i9form.pdf. It is the sole responsibility of the Contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any Contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on site performance under this contract. It is the Contractor's duty to assure that Contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that Contractor personnel may come into contact with.

H.6 2052.215-70 KEY PERSONNEL (JAN 1993)

(a) The following individuals are considered to be essential to the successful performance of the work hereunder:

Core Services (PSOW Section C.5)

Project Manager:	Floret Ikome
Integration Manager/ITI Architect:	Kenneth Griffin
Operations Manager:	Vince Longus
IT Security Operations & Compliance Manager:	Christopher Carter
Configuration/Asset Manager:	Santosh Vishwanathan
Transition and Quality Assurance Manager:	Philip Taylor
Service Desk Manager:	Al Mohning

Additional Services (PSOW Sections C.6.1, C.6.2, C.6.3, C.6.5, C.6.8, C.6.9)

Data Center Operations Manager:	Glenn Meyers
Incident Response Manager:	Ihsan Ul Haq
Software License Project Lead:	Eric Smith
Document Management Lead:	Kathleen Hornyak

The Contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this Section.

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less

effort to the work than indicated in the proposal or initially anticipated, the Contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution. The contracting officer and the project officer shall evaluate the Contractor's request and the contracting officer shall promptly notify the Contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the Contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

H.7 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL

a. NRC facilities may not be available due to (1) designated Federal holiday, any other day designated by Federal Statute, Executive Order, or by President's Proclamation; (2) early dismissal of NRC employees during working hours (e.g., special holidays, water emergency); or (3) occurrence of emergency conditions during nonworking hours (e.g., inclement weather).

b. When NRC facilities are unavailable, the Contractor's compensation and deduction policy (date), incorporated herein by reference, shall be followed for Contractor employees performing work on-site at the NRC facility. The Contractor shall promptly submit any revisions to this policy to the Contracting Officer for review before they are incorporated into the contract.

c. The Contractor shall not charge the NRC for work performed by on- site Contractor employees who were reassigned to perform other duties off site during the time the NRC facility was closed.

d. On-site Contractor staff shall be guided by the instructions given by a third party (e.g., Montgomery County personnel in situations which pose an immediate health or safety threat to employees (e.g., water emergency).

e. The Contractor's Project Director shall first consult the NRC Project Officer before authorizing leave for on-site personnel in situations which do not impose an immediate safety or health threat to employees (e.g., special holidays). That same day, the Contractor must then alert the Contracting Officer of the NRC Project Officer's direction. The Contractor shall continue to provide sufficient personnel to perform the requirements of essential tasks as defined in the Statement of Work which already are in operation or are scheduled.

H.8 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (JUL 2007)

The Contractor shall ensure that all its employees, subcontractor employees or consultants who are assigned to perform the work herein for contract performance for periods of more than 30 calendar days at NRC facilities, are approved by the NRC for unescorted NRC building access.

The Contractor shall conduct a preliminary federal facilities security screening interview or review for each of its employee, subcontractor employee, and consultants and submit to the NRC only the names of candidates for contract performance that have a reasonable probability of obtaining approval necessary for access to NRC's federal facilities. The Contractor shall pre- screen its applicants for the following:

(a) felony arrest in the last seven years; (b) alcohol related arrest within the last five years; (c) record of any military courts-martial convictions in the past 10 years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven years; (e) delinquency on any federal debts or bankruptcy in the last seven years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two copies of the pre-screening signed record or review shall be supplied to FSB/DFS with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all building access security applications required by this clause within ten business days of notification by FSB/DFS of initiation of the application process. Timely receipt of properly completed records of the Contractor's signed pre-screening record or review and building access security applications (submitted for candidates that have a reasonable probability of obtaining the level of security clearance necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

A Contractor, subcontractor employee or consultant shall not have access to NRC facilities until he/she is approved by FSB/DFS. Temporary access may be approved based on a favorable NRC review and discretionary determination of their building access security forms. Final building access will be approved based on favorably adjudicated checks by the Government. However, temporary access approval will be revoked and the Contractor's employee may subsequently be denied access in the event the employee's investigation cannot be favorably determined by the NRC. Such employee will not be authorized to work under any NRC contract requiring building access without the approval of FSB/DFS. When an individual receives final access, the individual will be subject to a review or reinvestigation every five years.

The Government will have and exercise full and complete control and discretion over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract at NRC facilities for a period of more than 30 calendar days shall be required to complete and submit to the Contractor representative an acceptable OPM Form 85P (Questionnaire for Public Trust Positions), and two FD 258 (Fingerprint Charts). Non-U.S. citizens must provide official documentation to the FSB/DFS, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U. S. Citizenship and Immigration Services. Any applicant with less than two years residency in the U. S. will not be approved for building access. The Contractor shall submit the documents to the NRC Project Officer (PO) who will give them to FSB/DFS.

FSB/DFS may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the OPM Form 85P and the Contractor's pre-screening record. Also, in the exercise of its authority, the Government may, among other things, grant or deny permanent building access approval based on the results of its review or investigation. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the NRC work sites for an extended period of time during the term of the contract. In the event that FSB/DFS are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the Contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The Contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

CANCELLATION OR TERMINATION OF BUILDING ACCESS/ REQUEST

The Contractor shall immediately notify the PO when a Contractor or su bContractor employee or consultant's need for NRC building access approval is withdrawn or the need by the Contractor employee's for building access terminates. The PO will immediately notify FSB/DFS (via e-mail) when a Contractor employee no longer requires building access. The Contractor shall be required to return any NRC issued badges to the Project Officer for return to FSB/DFS within three days after their termination.

H.9 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (JUL 2007)

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 and discretion over granting, denying, withholding, or terminating IT access approvals for individuals performing work under this contract.

The Contractor shall conduct a preliminary security interview or review for each IT level I or II access approval Contractor applicant and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of IT security access for which the candidate has been proposed. The Contractor shall pre-screen its applicants for the following:

(a) felony arrest in the last seven years; (b) alcohol related arrest within the last five years; (c) record of any military courts-martial convictions in the past ten years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven years; (e) delinquency on any federal debts or bankruptcy in the last seven years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two copies of the signed Contractor's pre-screening record or review will be supplied to FSB/DFS with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all IT access security applications required by this clause within ten business days of notification by FSB/DFS of initiation of the application process. Timely receipt of properly completed records of the pre-screening record and IT access security applications (submitted for candidates that have a reasonable probability of obtaining the level of security assurance necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

SECURITY REQUIREMENTS FOR IT 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.

A Contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary IT access may be approved based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved based on a favorably review or adjudication. However,

temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a reinvestigation every ten years.

The Contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 85P (Questionnaire for Public Trust Positions), two copies of the Contractor's signed pre-screening record and two FD 258 fingerprint charts, through the PO to FSB/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. Based on FSB/DFS review of the Contractor 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.

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) and SF- 85P 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 more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

SECURITY REQUIREMENTS FOR IT 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.

A Contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final IT access may be approved based on a favorably adjudication. However, temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a review or reinvestigation every ten years.

The Contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 85P (Questionnaire for Public Trust Positions), two copies of the Contractor's signed pre-screening record and two FD 258 fingerprint charts, through the PO to FSB/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. Based on FSB/DFS review of the Contractor 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.

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), SF- 85P, and Contractor's record of the pre-screening 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 more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for IT access is to be withdrawn or canceled, the Contractor shall immediately notify the PO by telephone in order that he/she will immediately contact FSB/DFS so that the access review 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 by the Contractor in writing to the PO who will forward the confirmation via email to FSB/DFS. Additionally, FSB/DFS must be immediately notified in writing 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 IT access.

H.10 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.

H.11 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.

H.12 COMPLIANCE WITH US IMMIGRATION LAWS AND REGULATIONS

NRC Contractors are responsible to ensure that their alien personnel are not in violation of United States Immigration and Naturalization (INS) laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form 1-151 or must present other evidence from the Immigration and Naturalization Services that employment will not affect his/her immigration status. The INS Office of Business Liaison (OBL) provides information to Contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on the INS website, http://www.ins.usdoj.gov/graphics/services/employerinfo/index.htm#obl.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC facilities or its equipment/services, and/or take any number of contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

H.13 SAFETY ON-SITE CONTRACTOR PERSONNEL

Ensuring the safety of occupants of Federal buildings is a responsibility shared by the professionals implementing our security and safety programs and the persons being protected. The NRC's Office of Administration (ADM) Division of Facilities and Security (DFS) has coordinated an Occupant Emergency Plan (OEP) for NRC Headquarters buildings with local authorities. The OEP has been approved by the Montgomery County Fire and Rescue Service. It is designed to improve building occupants' chances of survival, minimize damage to property, and promptly account for building occupants when necessary.

The Contractor's Project Director shall ensure that all personnel working full time on-site at NRC Headquarters read the NRC's OEP, provided electronically on the NRC Intranet at http://www.internal.nrc.gov/ADM/OEP.pdf The Contractor's Project Director also shall emphasize to each staff member that they are to be familiar with and guided by the OEP, as well as by instructions given by emergency response personnel in situations which pose an immediate health or safety threat to building occupants.

The NRC Project Officer shall ensure that the Contractor's Project Director has communicated the requirement for on-site Contractor staff to follow the guidance in the OEP. The NRC Project Officer also will assist in accounting for on-site contract persons in the event of a major emergency (e.g., explosion occurs and casualties or injuries are suspected) during which a full evacuation will be required, including the assembly and accountability of occupants. The NRC DFS will conduct drills periodically to train occupants and assess these procedures.

H.14 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2003)

NRC Contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day.

Contractor employees, consultants, and subcontractors shall complete the NRC's online, "Computer Security Awareness" course on the same day that they receive access to the agency's IT equipment and/or services, as their first action using the equipment/service. For those Contractor employees, consultants, and subcontractors who are already working under this contract, the on-line training must be completed in accordance with agency Network Announcements issued throughout the year 2003 within three weeks of issuance of this modification.

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the NRC throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC IT equipment and/or services, and/or take other appropriate contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

H.15 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (JULY 2006)

(a) The U.S. Nuclear Regulatory Commission (NRC) Contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC Contractor(s) and

subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24.

(b) Under this Whistleblower Employee Protection law, as implemented by regulations, NRC Contractor and subcontractor employees are protected from discharge, reprisal, threats, intimidation, coercion, blacklisting or other employment discrimination practices with respect to compensation, terms, conditions or privileges of their employment because the Contractor or subcontractor employee(s) has provided notice to the employer, refused to engage in unlawful practices, assisted in proceedings or testified on activities concerning alleged violations of the Atomic Energy Act of 1954 (as amended) and the Energy Reorganization Act of 1974 (as amended).

(c) The Contractor shall insert this or the substance of this clause in any subcontracts involving work performed under this contract.

H.16 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OVER CONTRACTOR

(a) For purposes of this clause, a foreign interest is defined as any of the following:

(1) A foreign Government or foreign Government agency;

(2) Any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) Any form of business enterprise organized or incorporated under the laws of the U.S., or a State or other jurisdiction within the U.S., which is owned, controlled, or influenced by a foreign Government, agency, firm, corporation or person; or

(4) Any person who is not a U.S. citizen.

(b) Foreign ownership, control, or influence (FOCI) may be present where the degree of ownership, control, or influence over a Contractor by a foreign interest is such that a reasonable basis exists for concluding that the compromise or unauthorized disclosure of classified information may occur.

(c) For purposes of this clause, subcontractor means any subcontractor at any tier and the term "contracting officer" shall mean NRC contracting officer. When this clause is included in a subcontract, the term "Contractor" shall mean subcontractor and the term "contract" shall mean subcontract.

(d) The Contractor shall immediately provide the contracting officer written notice of any changes in the extent and nature of FOCI over the Contractor which would affect the answers to the questions presented in DD Form 441S, "Certificate Pertaining to Foreign Interest". Further, notice of changes in ownership or control which are required to be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice shall also be furnished concurrently to the contracting officer.

(e) In those cases where a Contractor has changes involving FOCI, the NRC must determine whether the changes will pose an undue risk to the common defense and security. In making this determination, the contracting officer shall consider proposals made by the Contractor to avoid or mitigate foreign influences.

(f) The Contractor agrees to insert terms that conform substantially to the language of this clause including this paragraph (g) in all subcontracts under this contract that will require access to classified information. Additionally, the Contractor shall require such subcontractors to submit completed information required on the DD Form 441 form prior to award of a subcontract. Information to be provided by a subcontractor pursuant to this clause may be submitted directly to the contracting officer.

(g) Information submitted by the Contractor or any affected subcontractor as required pursuant to this clause shall be treated by NRC to the extent permitted by law, as business or financial information submitted in confidence to be used solely for purposes of evaluating FOCI.

(h) The requirements of this clause are in addition to the requirement that a Contractor obtain and retain the security clearances required by the contract. This clause shall not operate as a limitation on NRC's rights, including its rights to terminate this contract.

(i) The contracting officer may terminate this contract for default either if the Contractor fails to meet obligations imposed by this clause, e.g., provide the information required by this clause, comply with the contracting officer's instructions about safeguarding classified information, or make this clause applicable to subcontractors, or if, in the contracting officer's judgment, the Contractor creates a FOCI situation in order to avoid performance or a termination for default. The contracting officer may terminate this contract for convenience if the Contractor becomes subject to FOCI and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the FOCI problem.

H.17 2052.204.70 SECURITY (MAR 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 sensitive unclassified information (e.g., Safeguards), 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, or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, 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 shall 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.

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.

H.18 PROJECT SUPPORT CONTRACTORS

The Government may either award or have awarded management, engineering, technical, and other professional support service contracts (hereafter referred to as Project Support Contractors). Project Support Contractors may require access to proprietary and other data relating to technical matters (including cost and schedule) concerning this contract to the same degree such access is accorded Government personnel.

The Contractor shall cooperate with Project Support Contractors by engaging in technical discussions with Project Support Contractors' personnel, and permitting such personnel access to information and data relating to technical matters (including cost and schedule) concerning this contract to the same degree such access is accorded Government personnel.

Project Support Contractors shall agree to protect proprietary information of the Contractor in accordance with Federal Acquisition Regulation (FAR) 9.505-4, to not engage in the production of products (including software), and to otherwise abide by FAR Subpart 9.5, entitled "Organizational Conflicts of Interest." Project Support Contractors shall be required to directly execute nondisclosure, non-use agreements with the Contractor and subcontractors if so requested by the Contractor.

H.19 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following contract clauses pertinent to this Section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract. See www.acquisition.gov/far for electronic access to the full text of a clause.

NUMBER	TITLE FEDERAL ACQUISITION REGULATION	DATE
52.249-14	EXCUSABLE DELAYS	APR 1984
52.227-17	RIGHTS IN DATA – SPECIAL WORKS	DEC 2007

H.20 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (MAY 2009)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104 (g)).

(2) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77, 108-78)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[X] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

[X] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (DEC 2008)(Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

[] (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (MAR 2009) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[] (4) 52.204-11, American Recovery and Reinvestment Act-Reporting Requirements (MAR 2009) (Pub. L. 111-5).

[] (5) 52.219-3, Notice of Total HUBZone Set-Aside (Jan 1999) (15 U.S.C. 657a).

[] (6) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (July 2005) (if the Offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[] (7) [Reserved]

[] (8)(i) 52.219-6, Notice of Total Small Business Set-Aside (June 2003) (15 U.S.C. 644).

[] (ii) Alternate I (Oct 1995) of 52.219-6.

[] (iii) Alternate II (Mar 2004) of 52.219-6.

[] (9)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

[] (ii) Alternate I (Oct 1995) of 52.219-7.

[] (iii) Alternate II (Mar 2004) of 52.219-7.

[X] (10) 52.219-8, Utilization of Small Business Concerns (May 2004) (15 U.S.C. 637(d)(2) and (3)).

[] (11)(i) 52.219-9, Small Business Subcontracting Plan (APR 2008) (15 U.S.C. 637(d)(4)).

[] (ii) Alternate I (Oct 2001) of 52.219-9.

[X] (iii) Alternate II (Oct 2001) of 52.219-9.

[] (12) 52.219-14, Limitations on Subcontracting (Dec 1996) (15 U.S.C. 637(a)(14)).

[X] (13) 52.219-16, Liquidated Damages--Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[] (14)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the Offeror elects to waive the adjustment, it shall so indicate in its offer.)

[] (ii) Alternate I (June 2003) of 52.219-23.

[] (15) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (APR 2008) (Pub. L. 103-355, Section 7102, and 10 U.S.C. 2323).

[] (16) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (Oct 2000) Pub. L. 103-355, Section 7102, and 10 U.S.C. 2323).

[] (17) 52.219-27, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (May 2004) (15 U.S.C. 657 f).

[] (18) 52.219-28, Post Award Small Business Program Representation (APR 2009) (15 U.S.C 632(a)(2)).

[X] (19) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

[] (20) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (FEB 2008) (E.O. 13126).

[X] (21) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

[X] (22) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

[X] (23) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sept 2006) (38 U.S.C. 4212).

[X] (24) 52.222-36, Affirmative Action for Workers with Disabilities (Jun 1998) (29 U.S.C. 793).

[X] (25) 52.222-37, Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sept 2006) (38 U.S.C. 4212).

[X] (26) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

[X] (27) 52.222-54, Employment Eligibility Verification (Jan 2009). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[] (28)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[X] (29) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

[X] (30)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).

[] (ii) Alternate I (DEC 2007) of 52.223-16.

[] (31) 52.225-1, Buy American Act--Supplies (FEB 2009) (41 U.S.C. 10a-10d).

[] (32)(i) 52.225-3, Buy American Act--Free Trade Agreements-- Israeli Trade Act (FEB 2009) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, Pub. L 108-77, 108-78, 108-286, 109-53 and 109-169).

[] (ii) Alternate I (Jan 2004) of 52.225-3.

[] (iii) Alternate II (Jan 2004) of 52.225-3.

[X] (33) 52.225-5, Trade Agreements (MAR 2009) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

[X] (34) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[] (35) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

[] (36) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

[] (37) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (38) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[X] (39) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (Oct 2003) (31 U.S.C. 3332).

[] (40) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (May 1999) (31 U.S.C. 3332).

[] (41) 52.232-36, Payment by Third Party (May 1999) (31 U.S.C. 3332).

[] (42) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

[] (43)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

[] (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[] (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

[] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (Nov 2006) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Feb 2002) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

[] (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

[] (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247)

[] (8) 52.237-11, Accepting and Dispensing of $1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (DEC 2008) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (May 2004) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (Sept 2006) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (June 1998) (29 U.S.C. 793).

(vii) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (Dec 2004) (E.O. 13201).

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements "(Nov 2007)" (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (FEB 2009)(41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employee Eligibility Verification (JAN 2009)

(xiii) 52.226-6, Promoting Excess Food Donataion to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

H.21 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of expiration of the then-current term; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed six (6) years.

H.22 2052.209-72 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST (JAN 1993)

(a) Purpose. The primary purpose of this clause is to aid in ensuring that the Contractor:

(1) Is not placed in a conflicting role because of current or planned interests (financial, contractual, organizational, or otherwise) which relate to the work under this contract; and

(2) Does not obtain an unfair competitive advantage over other parties by virtue of its performance of this contract.

(b) Scope. The restrictions described apply to performance or participation by the Contractor, as defined in 48 CFR 2009.570-2 in the activities covered by this clause.

(c) Work for others.

(1) Notwithstanding any other provision of this contract, during the term of this contract, the Contractor agrees to forego entering into consulting or other contractual arrangements with any firm or organization the result of which may give rise to a conflict of interest with respect to the work being performed under this contract. The Contractor shall ensure that all employees under this contract abide by the provision of this clause. If the Contractor has reason to believe, with respect to itself or any employee, that any proposed consultant or other contractual arrangement with any firm or organization may involve a potential conflict of interest, the Contractor shall obtain the written approval of the contracting officer before the execution of such contractual arrangement.

(2) The Contractor may not represent, assist, or otherwise support an NRC licensee or applicant undergoing an NRC audit, inspection, or review where the activities that are the subject of the audit, inspection, or review are the same as or substantially similar to the services within the scope of this contract (or task order as appropriate) except where the NRC licensee or applicant requires the Contractor's support to explain or defend the Contractor's prior work for the utility or other entity which NRC questions.

(3) When the Contractor performs work for the NRC under this contract at any NRC licensee or applicant site, the Contractor shall neither solicit nor perform work in the same or similar technical area for that licensee or applicant organization for a period commencing with the award of the task order or beginning of work on the site (if not a task

order contract) and ending one year after completion of all work under the associated task order, or last time at the site (if not a task order contract).

(4) When the Contractor performs work for the NRC under this contract at any NRC licensee or applicant site,

(i) The Contractor may not solicit work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate.

(ii) The Contractor may not perform work at that site for that licensee or applicant during the period of performance of the task order or the contract, as appropriate, and for one year thereafter.

(iii) Notwithstanding the foregoing, the contracting officer may authorize the Contractor to solicit or perform this type of work (except work in the same or similar technical area) if the contracting officer determines that the situation will not pose a potential for technical bias or unfair competitive advantage.

(d) Disclosure after award.

(1) The Contractor warrants that to the best of its knowledge and belief, and except as otherwise set forth in this contract, that it does not have any organizational conflicts of interest as defined in 48 CFR 2009.570-2.

(2) The Contractor agrees that if, after award, it discovers organizational conflicts of interest with respect to this contract, it shall make an immediate and full disclosure in writing to the contracting officer. This statement must include a description of the action which the Contractor has taken or proposes to take to avoid or mitigate such conflicts. The NRC may, however, terminate the contract if termination is in the best interest of the Government.

(3) It is recognized that the scope of work of a task-order-type contract necessarily encompasses a broad spectrum of activities. Consequently, if this is a task-order-type contract, the Contractor agrees that it will disclose all proposed new work involving NRC licensees or applicants which comes within the scope of work of the underlying contract. Further, if this contract involves work at a licensee or applicant site, the Contractor agrees to exercise diligence to discover and disclose any new work at that licensee or applicant site. This disclosure must be made before the submission of a bid or proposal to the utility or other regulated entity and must be received by the NRC at least 15 days before the proposed award date in any event, unless a written justification demonstrating urgency and due diligence to discover and disclose is provided by the Contractor and approved by the contracting officer. The disclosure must include the Statement of Work, the dollar value of the proposed contract, and any other documents that are needed to fully describe the proposed work for the regulated utility or other regulated entity. NRC may deny approval of the disclosed work only when the NRC has issued a task order which includes the technical area and, if site-specific, the site, or has plans to issue a task order which includes the technical area and, if site-specific, the site, or when the work violates paragraphs (c)(2), (c)(3) or (c)(4) of this Section.

(e) Access to and use of information.

(1) If in the performance of this contract, the Contractor obtains access to information, such as NRC plans, policies, reports, studies, financial plans, internal data protected by the Privacy Act of 1974 (5 U.S.C. Section 552a (1988)), or the Freedom of Information Act (5 U.S.C. Section 552 (1986)), the Contractor agrees not to:

(i) Use this information for any private purpose until the information has been released to the public;

(ii) Compete for work for the Commission based on the information for a period of six months after either the completion of this contract or the release of the information to the public, whichever is first;

(iii) Submit an unsolicited proposal to the Government based on the information until one year after the release of the information to the public; or

(iv) Release the information without prior written approval by the contracting officer unless the information has previously been released to the public by the NRC.

(2) In addition, the Contractor agrees that, to the extent it receives or is given access to proprietary data, data protected by the Privacy Act of 1974 (5 U.S.C. Section 552a (1988)), or the Freedom of Information Act (5 U.S.C. Section 552 (1986)), or other confidential or privileged technical, business, or financial information under this contract, the Contractor shall treat the information in accordance with restrictions placed on use of the information.

(3) Subject to patent and security provisions of this contract, the Contractor shall have the right to use technical data it produces under this contract for private purposes provided that all requirements of this contract have been met.

(f) Subcontracts. Except as provided in 48 CFR 2009.570-2, the Contractor shall include this clause, including this paragraph, in subcontracts of any tier. The terms contract, Contractor, and contracting officer, must be appropriately modified to preserve the Government's rights.

(g) Remedies. For breach of any of the above restrictions, or for intentional nondisclosure or misrepresentation of any relevant interest required to be disclosed concerning this contract or for such erroneous representations that necessarily imply bad faith, the Government may terminate the contract for default, disqualify the Contractor from subsequent contractual efforts, and pursue other remedies permitted by law or this contract.

(h) Waiver. A request for waiver under this clause must be directed in writing to the contracting officer in accordance with the procedures outlined in 48 CFR 2009.570-9.

(i) Follow-on effort. The Contractor shall be ineligible to participate in NRC contracts, subcontracts, or proposals therefore (solicited or unsolicited), which stem directly from the Contractor's performance of work under this contract. Furthermore, unless so directed in writing by the contracting officer, the Contractor may not perform any technical consulting or management support services work or evaluation activities under this contract on any of its products or services or the products or services of another firm if the Contractor has been substantially involved in the development or marketing of the products or services.

(1) If the Contractor, under this contract, prepares a complete or essentially complete Statement of Work or specifications, the Contractor is not eligible to perform or participate in the initial contractual effort which is based on the Statement of Work or specifications. The Contractor may not incorporate its products or services in the Statement of Work or specifications unless so directed in writing by the contracting officer, in which case the restrictions in this paragraph do not apply.

(2) Nothing in this paragraph precludes the Contractor from offering or selling its standard commercial items to the Government.

H.23 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION OR PERFORMING IN ESPECIALLY SENSITIVE POSITIONS

NRC's Headquarters Assistant Drug Program Coordinator (ADPC) shall be responsible for implementing and managing the collecting and testing portions of the NRC Contractor Drug Testing Program. The Headquarters ADPC function is carried out by the Drug Program Manager in the Division of Facilities and Security, Office of Administration. All sample collection, testing, and review of test results shall be conducted by the NRC "drug testing Contractor." The NRC will reimburse the NRC "drug testing Contractor" for these services.

All Contractor employees, subcontractor employees, and consultants proposed for performance or performing under this contract shall be subject to the requirements of the clause if they meet one of the following criteria stated in the Plan: (1) individuals who require unescorted access to nuclear power plants, (2) individuals who have access to classified or safeguards information, (3) individuals who are required to carry firearms in performing security services

for the NRC, (4) individuals who are required to operate Government vehicles or transport passengers for the NRC, (5) individuals who are required to operate hazardous equipment at NRC facilities, or (6) individuals who admit to recent illegal drug use or those who are found through other means
to be using drugs illegally. The Plan includes pre-assignment, random, reasonable suspicion, and post-accident drug testing. The due process procedures applicable to NRC employees under NRC=s Drug Testing Program are not applicable to Contractors, consultants, subcontractors and their employees. Rather, a Contractor's employees and their subcontractors are subject to the procedures and terms of their employment agreements with their employer.

The NRC Drug Program Manager will schedule the drug testing for all Contractor employees, subcontractor employees, and consultants who are subject to testing under this clause in accordance with the Plan. The NRC will reimburse the NRC "drug testing Contractor" for collecting, testing, and reviewing test results. Any NRC Contractor found to be using, selling, or possessing illegal drugs, or any Contractor with a verified positive drug test result under this program while in a duty status will immediately be removed from working under the NRC contract. The Contractor's employer will be notified of the denial or revocation of the individual's authorization to have access to information and ability to perform under the contract. The individual may not work on any NRC contract for a period of not less than one year from the date of the failed drug test and will not be considered for reinstatement unless evidence of rehabilitation, as determined by the NRC "drug testing Contractor's" Medical Review Officer, is provided.

Contractor drug testing records are protected under the NRC Privacy Act Systems of Records, System 35, "Drug Testing Program Records - NRC" (copy enclosed).

H.24 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by a warranted NRC Contracting Officer. Such orders may be issued for thirty-six months from the date of award specified in Section C.5., and for three additional twelve month option periods (if options are exercised)

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

H.25 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $50,000.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor:

(1) Any order for a single item in excess of $30,000,000.00.

(2) Any order for a combination of items in excess of $30,000,000.00.

(3) A series of orders from the same ordering office within 30 days that together call for quantities exceeding the imitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

H.26 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract beyond 180 days after the end of the contract.

H.27 52.237-3 CONTINUITY OF SERVICES (Jan 1991)

(a) The Contractor recognizes that the services under this contract are vital to the Government and must be continued without interruption and that, upon contract expiration, a successor, either the Government or another contractor, may continue them. The Contractor agrees to –

(1) Furnish phase-in training; and

(2) Exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor.

(b) The Contractor shall, upon the Contracting Officer's written notice,

(1) furnish phase-in, phase-out services for up to 90 days after this contract expires and

(2) negotiate in good faith a plan with a successor to determine the nature and extent of phase-in, phase-out services required.

The plan shall specify a training program and a date for transferring responsibilities for each division of work described in the plan, and shall be subject to the Contracting Officer's approval. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the services called for by this contract are maintained at the required level of proficiency.

(c) The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

(d) The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after contract expiration that result from phase-in, phase-out operations) and a fee (profit) not to exceed a pro rata portion of the fee (profit) under this contract.

PART II - CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

I.1 NOTICE OF ALLOWABLE CONTRACT TYPES

This is an IDIQ contract. See the listing below for applicable contract types for requirements:

FFP = Firm-Fixed-Price
LH = Labor-Hour

When applicable, the following symbols will appear next to the applicable clauses and provisions throughout this document.

$ = applicable to FIRM-FIXED-PRICE line items only.

& = applicable to LABOR-HOUR line items only.

I.2 52.223-2 AFFIRMATIVE PROCUREMENT OF BIOBASED PRODUCTS UNDER SERVICE AND CONSTRUCTION CONTRACTS (DEC 2007)

(a) In the performance of this contract, the contractor shall make maximum use of biobased products that are United States Department of Agriculture (USDA)-designated items unless--

(1) The product cannot be acquired--

(i) Competitively within a time frame providing for compliance with the contract performance schedule;

(ii) Meeting contract performance requirements; or

(iii) At a reasonable price.

(2) The product is to be used in an application covered by a USDA categorical exemption (see 7 CFR 2902.10 et seq.). For example, some USDA-designated items such as mobile equipment hydraulic fluids, diesel fuel additives, and penetrating lubricants are excluded from the preferred procurement requirement for the application of the USDA-designated item to one or both of the following:

(i) Spacecraft system and launch support equipment.

(ii) Military equipment, i.e., a product or system designed or procured for combat or combat-related missions.

(b) Information about this requirement and these products is available at http://www.usda.gov/biopreferred.

I.3 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond those specified in individual orders. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond limitations specified in individual orders, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

ATTACHMENT	TITLE
A	STATEMENT OF WORK/SPECIFICATION
B	BILLING INSTRUCTIONS LABOR HOUR
C	BILLING INSTRUCTIONS FIXED PRICE
D	PRICE SCHEDULE
E	NRC 187
F	OCOI Guidelines
G	NRC-Approved Small Business Subcontracting Plan

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

General: During performance and through final payment of this contract, the contractor is responsible for the accuracy and completeness of 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/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

Form: Claims shall be submitted on the payee's letterhead, voucher/invoice, 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."

Number of Copies: A signed original shall be submitted. If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original is also required.

Designated Agency Billing Office: The preferred method of submitting vouchers/invoices is electronically to the Department of the Interior at NRCPayments@nbc.gov

If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be electronically sent to: Property@nrc.gov

However, if you submit a hard-copy of the voucher/invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

If you submit a hard-copy of the voucher/invoice and it includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be mailed to the following address:

U.S. Nuclear Regulatory Commission
NRC Property Management Officer
Mail Stop: O-4D15
Washington, DC 20555-0001

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of Standard Form 26, Block 25 of Standard Form 33, or Block 18a. of Standard Form 1449, whichever is applicable.

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

Frequency: The contractor shall submit claims for reimbursement once each month, unless otherwise authorized by the Contracting Officer.

Format: Claims shall be submitted in the format depicted on the attached sample form entitled "Voucher/Invoice for Purchases and Services Other than Personal" (see Attachment 1). The sample format is provided for guidance only. The format is not required for submission of a voucher/invoice. Alternate formats are permissible provided all requirements of the billing instructions are addressed.

Billing of Cost after Expiration of Contract: If costs are incurred during the contract period and claimed after the contract has expired, you must cite the period during which these costs were incurred. To be considered a proper expiration voucher/invoice, the contractor shall clearly mark it "EXPIRATION VOUCHER" or "EXPIRATION INVOICE".

Final vouchers/invoices 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.

R:txtselden\billing instructions LH or TM revised 2008

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL (SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

2. Voucher Information

a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee'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 Payee to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.

b. 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).

c. Contract Number. Insert the NRC contract number.

d. Voucher/Invoice. The appropriate sequential number of the voucher/invoice, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.

e. Date of Voucher/Invoice. Insert the date the voucher/invoice is prepared.

f. Billing period. Insert the beginning and ending dates (day, month, and year) of the period during which costs were incurred and for which reimbursement is claimed.

g. Required Attachments (Supporting Documentation). Direct Costs. The contractor shall submit as an attachment to its invoice/voucher cover sheet a listing of labor categories, hours billed, fixed hourly rates, total dollars, and cumulative hours billed to date under each labor category authorized under the contract/purchase order for each of the activities to be performed under the contract/purchase order. The contractor shall include incurred costs for: (1) travel, (2) materials, including non-capitalized equipment and supplies, (3) capitalized nonexpendable equipment, (4) materials handling fee, (5) consultants (supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval), and (6) subcontracts (include separate detailed breakdown of all costs paid to approved subcontractors during the billing period) with the required supporting documentation, as well as the cumulative total of each cost, billed to date by activity.

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

3. Definitions

a. Non-capitalized Equipment, Materials, and Supplies. These are equipment other than that described in number (4) below, plus consumable materials, supplies. List by category. List items valued at $1,000 or more separately. Provide the item number for each piece of equipment valued at $1,000 or more.

b. Capitalized Non Expendable Equipment. List each item costing $50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) the item number for the specific piece of equipment listed in the property schedule of the contract; or (b) the Contracting Officer's approval letter if the equipment is not covered by the property schedule.

c. Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures.

Sample Voucher Information (Supporting Documentation must be attached)

This voucher/invoice represents reimbursable costs for the billing period from _____ through _____.

		Amount Billed	
		Current Period	Cumulative
(f)	Direct Costs:		
	(1) Direct Labor	$_____	$_____
	(2) Travel	$_____	$_____
	(3) Materials	$_____	$_____
	(4) Equipment	$_____	$_____
	(5) Materials Handling Fee	$_____	$_____
	(6) Consultants	$_____	$_____
	(7) Subcontracts	$_____	$_____
	Total Direct Costs:	$_____	$_____

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

General: During performance and through final payment of this contract, the contractor is responsible for the accuracy and completeness of 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/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

Form: Claims shall be submitted on the payee's letterhead, voucher/invoice, 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."

Number of Copies: A signed original shall be submitted. If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original is also required.

Designated Agency Billing Office: The preferred method of submitting vouchers/invoices is electronically to the Department of the Interior at NRCPayments@nbc.gov

If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be electronically sent to: Property@nrc.gov

However, if you submit a hard-copy of the voucher/invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

If you submit a hard-copy of the voucher/invoice and it includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be mailed to the following address:

U.S. Nuclear Regulatory Commission
NRC Property Management Officer
Mail Stop: O-4D15
Washington, DC 20555-0001

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of Standard Form 26, Block 25 of Standard Form 33, or Block 18a. of Standard Form 1449, whichever is applicable.

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

Frequency: The contractor shall submit claims for reimbursement once each month, unless otherwise authorized by the Contracting Officer.

Format: Claims shall be submitted in the format depicted on the attached sample form entitled "Voucher/Invoice for Purchases and Services Other than Personal" (see Attachment 1). The sample format is provided for guidance only. The format is not required for submission of a voucher/invoice. Alternate formats are permissible provided all requirements of the billing instructions are addressed.

Billing of Cost after Expiration of Contract: If costs are incurred during the contract period and claimed after the contract has expired, you must cite the period during which these costs were incurred. To be considered a proper expiration voucher/invoice, the contractor shall clearly mark it "EXPIRATION VOUCHER" or "EXPIRATION INVOICE".

Final vouchers/invoices 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.

R:txtselden\billing instructions LH or TM revised 2008

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL (SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

2. Voucher Information

a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee'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 Payee to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.

b. 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).

c. Contract Number. Insert the NRC contract number.

d. Voucher/Invoice. The appropriate sequential number of the voucher/invoice, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.

e. Date of Voucher/Invoice. Insert the date the voucher/invoice is prepared.

f. Billing period. Insert the beginning and ending dates (day, month, and year) of the period during which costs were incurred and for which reimbursement is claimed.

g. Required Attachments (Supporting Documentation). Direct Costs. The contractor shall submit as an attachment to its invoice/voucher cover sheet a listing of labor categories, hours billed, fixed hourly rates, total dollars, and cumulative hours billed to date under each labor category authorized under the contract/purchase order for each of the activities to be performed under the contract/purchase order. The contractor shall include incurred costs for: (1) travel, (2) materials, including non-capitalized equipment and supplies, (3) capitalized nonexpendable equipment, (4) materials handling fee, (5) consultants (supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval), and (6) subcontracts (include separate detailed breakdown of all costs paid to approved subcontractors during the billing period) with the required supporting documentation, as well as the cumulative total of each cost, billed to date by activity.

ATTACHMENT B

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008)

3. Definitions

a. Non-capitalized Equipment, Materials, and Supplies. These are equipment other than that described in number (4) below, plus consumable materials, supplies. List by category. List items valued at $1,000 or more separately. Provide the item number for each piece of equipment valued at $1,000 or more.

b. Capitalized Non Expendable Equipment. List each item costing $50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) the item number for the specific piece of equipment listed in the property schedule of the contract; or (b) the Contracting Officer's approval letter if the equipment is not covered by the property schedule.

c. Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures.

Sample Voucher Information (Supporting Documentation must be attached)

This voucher/invoice represents reimbursable costs for the billing period from_____through_____.

		Amount Billed	
		Current Period	Cumulative
(f)	Direct Costs:		
	(1) Direct Labor	$_____	$_____
	(2) Travel	$_____	$_____
	(3) Materials	$_____	$_____
	(4) Equipment	$_____	$_____
	(5) Materials Handling Fee	$_____	$_____
	(6) Consultants	$_____	$_____
	(7) Subcontracts	$_____	$_____
	Total Direct Costs:	$_____	$_____

ATTACHMENT C

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

General: During performance and through final payment of this contract, the contractor is responsible for the accuracy and completeness of 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/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

Form: Claims shall be submitted on the payee's letterhead, voucher/invoice, 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."

Number of Copies: A signed original shall be submitted. If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original is also required.

Designated Agency Billing Office: The preferred method of submitting vouchers/invoices is electronically to the Department of the Interior at NRCPayments@nbc.gov

If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be electronically sent to: Property@nrc.gov

However, if you submit a hard-copy of the voucher/invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

If you submit a hard-copy of the voucher/invoice and it includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be mailed to the following address:

U.S. Nuclear Regulatory Commission
NRC Property Management Officer
Mail Stop: O-4D15
Washington, DC 20555-0001

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of the Standard Form 26, Block 25 of the Standard Form 33, or Block 18a. of the Standard Form 1449, whichever is applicable.

Frequency: The contractor shall submit a voucher/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. A description of articles or services, quantity, unit price, and total amount.

7. For contractor acquired property, list each item with an initial acquisition cost of $50,000 or more 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.

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

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.

Attachment G

NRCAR Subpart 2009.5 Organizational Conflicts of Interest

§2009.500 Scope of subpart.

In accordance with 42 U.S.C. 2210a., NRC acquisitions are processed in accordance with §2009.570, which takes precedence over FAR 9.5 with respect to organizational conflicts of interest. Where non-conflicting guidance appears in FAR 9.5, that guidance must be followed.

§2009.570 NRC organizational conflicts of interest.

§2009.570-1 Scope of policy.

(a) It is the policy of NRC to avoid, eliminate, or neutralize contractor organizational conflicts of interest. The NRC achieves this objective by requiring all prospective contractors to submit information describing relationships, if any, with organizations or persons (including those regulated by the NRC) which may give rise to actual or potential conflicts of interest in the event of contract award.

(b) Contractor conflict of interest determinations cannot be made automatically or routinely. The application of sound judgment on virtually a case-by-case basis is necessary if the policy is to be applied to satisfy the overall public interest. It is not possible to prescribe in advance a specific method or set of criteria which would serve to identify and resolve all of the contractor conflict of interest situations that might arise. However, examples are provided in these regulations to guide application of this policy guidance. The ultimate test is as follows: Might the contractor, if awarded the contract, be placed in a position where its judgment may be biased, or where it may have an unfair competitive advantage?

(c) The conflict of interest rule contained in this subpart applies to contractors and offerors only. Individuals or firms who have other relationships with the NRC (e.g., parties to a licensing proceeding) are not covered by this regulation. This rule does not apply to the acquisition of consulting services through the personnel appointment process, NRC agreements with other Government agencies, international organizations, or state, local, or foreign Governments. Separate procedures for avoiding conflicts of interest will be employed in these agreements, as appropriate.

§2009.570-2 Definitions.

Affiliates means business concerns which are affiliates of each other when either directly or indirectly one concern or individual controls or has the power to control another, or when a third party controls or has the power to control both.

Contract means any contractual agreement or other arrangement with the NRC except as provided in §2009.570-1(c).

Contractor means any person, firm, unincorporated association, joint venture, co-sponsor, partnership, corporation, affiliates thereof, or their successors in interest, including their chief executives, directors, key personnel (identified in the contract), proposed consultants or subcontractors, which are a party to a contract with the NRC.

Evaluation activities means any effort involving the appraisal of a technology, process, product, or policy.

Offeror or prospective contractor means any person, firm, unincorporated association, joint venture, co-sponsor, partnership, corporation, or their affiliates or successors in interest, including their chief executives, directors, key personnel, proposed consultants, or subcontractors, submitting a bid or proposal, solicited or unsolicited, to the NRC to obtain a contract.

Organizational conflicts of interest means that a relationship exists whereby a contractor or prospective contractor has present or planned interests related to the work to be performed under an NRC contract which:

(1) May diminish its capacity to give impartial, technically sound, objective assistance and advice, or may otherwise result in a biased work product; or

(2) May result in its being given an unfair competitive advantage.

Potential conflict of interest means that a factual situation exists that suggests that an actual conflict of interest may arise from award of a proposed contract. The term potential conflict of interest is used to signify those situations that

(1) Merit investigation before contract award to ascertain whether award would give rise to an actual conflict; or

(2) Must be reported to the contracting officer for investigation if they arise during contract performance.

Research means any scientific or technical work involving theoretical analysis, exploration, or experimentation.

Subcontractor means any subcontractor of any tier who performs work under a contract with the NRC except subcontracts for supplies and subcontracts in amounts not exceeding $10,000.

Technical consulting and management support services means internal assistance to a component of the NRC in the formulation or administration of its programs, projects, or policies which normally require that the contractor be given access to proprietary information or to information that has not been made available to the public. These services typically include assistance in the preparation of program plans, preliminary designs, specifications, or statements of work.

§2009.570-3 Criteria for recognizing contractor organizational conflicts of interest.

(a) General.

(1) Two questions will be asked in determining whether actual or potential organizational conflicts of interest exist:

(i) Are there conflicting roles which might bias an offeror's or contractor's judgment in relation to its work for the NRC?

(ii) May the offeror or contractor be given an unfair competitive advantage based on the performance of the contract?

(2) NRC's ultimate determination that organizational conflicts of interest exist will be made in light of common sense and good business judgment based upon the relevant facts. While it is difficult to identify and to prescribe in advance a specific method for avoiding all of the various situations or relationships that might involve potential organizational conflicts of interest, NRC personnel will pay particular attention to proposed contractual requirements that call for the rendering of advice, consultation or evaluation activities, or similar activities that directly lay the groundwork for the NRC's decisions on regulatory activities, future procurements, and research programs. Any work performed at an applicant or licensee site will also be closely scrutinized by the NRC staff.

(b) Situations or relationships. The following situations or relationships may give rise to organizational conflicts of interest:

(1) The offeror or contractor shall disclose information that may give rise to organizational conflicts of interest under the following circumstances. The information may include the scope of work or specification for the requirement being performed, the period of performance, and the name and telephone number for a point of contact at the organization knowledgeable about the commercial contract.

(i) Where the offeror or contractor provides advice and recommendations to the NRC in the same technical area where it is also providing consulting assistance to any organization regulated by the NRC.

(ii) Where the offeror or contractor provides advice to the NRC on the same or similar matter on which it is also providing assistance to any organization regulated by the NRC.

(iii) Where the offeror or contractor evaluates its own products or services, or has been substantially involved in the development or marketing of the products or services of another entity.

(iv) Where the award of a contract would result in placing the offeror or contractor in a conflicting role in which its judgment may be biased in relation to its work for the NRC, or would result in an unfair competitive advantage for the offeror or contractor.

(v) Where the offeror or contractor solicits or performs work at an applicant or licensee site while performing work in the same technical area for the NRC at the same site.

(2) The contracting officer may request specific information from an offeror or contractor or may require special contract clauses such as provided in §2009.570-5(b) in the following circumstances:

(i) Where the offeror or contractor prepares specifications that are to be used in competitive procurements of products or services covered by the specifications.

(ii) Where the offeror or contractor prepares plans for specific approaches or methodologies that are to be incorporated into competitive procurements using the approaches or methodologies.

(iii) Where the offeror or contractor is granted access to information not available to the public concerning NRC plans, policies, or programs that could form the basis for a later procurement action.

(iv) Where the offeror or contractor is granted access to proprietary information of its competitors.

(v) Where the award of a contract might result in placing the offeror or contractor in a conflicting role in which its judgment may be biased in relation to its work for the NRC or might result in an unfair competitive advantage for the offeror or contractor.

(c) Policy application guidance. The following examples are illustrative only and are not intended to identify and resolve all contractor organizational conflict of interest situations.

(1)(i) Example. The ABC Corp., in response to a Request For Proposal (RFP), proposes to undertake certain analyses of a reactor component as called for in the RFP. The ABC Corp. is one of several companies considered to be technically well qualified. In response to the inquiry in the RFP, the ABC Corp. advises that it is currently performing similar analyses for the reactor manufacturer.

(ii) Guidance. An NRC contract for that particular work normally would not be awarded to the ABC Corp. because the company would be placed in a position in which its judgment could be biased in relationship to its work for the NRC. Because there are other well-qualified companies available, there would be no reason for considering a waiver of the policy.

(2)(i) Example. The ABC Corp., in response to an RFP, proposes to perform certain analyses of a reactor component that is unique to one type of advanced reactor. As is the case with other technically qualified companies responding to the RFP, the ABC Corp. is performing various projects for several different utility clients. None of the ABC Corp. projects have any relationship to the work called for in the RFP. Based on the NRC evaluation, the ABC Corp. is considered to be the best qualified company to perform the work outlined in the RFP.

(ii) Guidance. An NRC contract normally could be awarded to the ABC Corp. because no conflict of interest exists which could motivate bias with respect to the work. An appropriate clause would be included in the contract to preclude the ABC Corp. from subsequently contracting for work with the private sector that could create a conflict during the performance of the NRC contract. For example, ABC Corp. would be precluded from the performance of similar work for the company developing the advanced reactor mentioned in the example.

(3)(i) Example. The ABC Corp., in response to a competitive RFP, submits a proposal to assist the NRC in revising NRC's guidance documents on the respiratory protection requirements of 10 CFR Part 20. ABC Corp. is the only firm determined to be technically acceptable. ABC Corp. has performed substantial work for regulated utilities in the past and is expected to continue

similar efforts in the future. The work has and will cover the writing, implementation, and administration of compliance respiratory protection programs for nuclear power plants.

(ii) Guidance. This situation would place the firm in a role where its judgment could be biased in relationship to its work for the NRC. Because the nature of the required work is vitally important in terms of the NRC's responsibilities and no reasonable alternative exists, a waiver of the policy, in accordance with §2009.570-9 may be warranted. Any waiver must be fully documented in accordance with the waiver provisions of this policy with particular attention to the establishment of protective mechanisms to guard against bias.

(4)(i) Example. The ABC Corp. submits a proposal for a new system to evaluate a specific reactor component's performance for the purpose of developing standards that are important to the NRC program. The ABC Corp. has advised the NRC that it intends to sell the new system to industry once its practicability has been demonstrated. Other companies in this business are using older systems for evaluation of the specific reactor component.

(ii) Guidance. A contract could be awarded to the ABC Corp. if the contract stipulates that no information produced under the contract will be used in the contractor's private activities unless this information has been reported to the NRC. Data on how the reactor component performs, which is reported to the NRC by contractors, will normally be disseminated by the NRC to others to preclude an unfair competitive advantage. When the NRC furnishes information about the reactor component to the contractor for the performance of contracted work, the information may not be used in the contractor's private activities unless the information is generally available to others. Further, the contract will stipulate that the contractor will inform the NRC contracting officer of all situations in which the information, developed about the performance of the reactor component under the contract, is proposed to be used.

(5)(i) Example. The ABC Corp., in response to a RFP, proposes to assemble a map showing certain seismological features of the Appalachian fold belt. In accordance with the representation in the RFP and §2009.570-3(b)(1)(i), ABC Corp. informs the NRC that it is presently doing seismological studies for several utilities in the eastern United States, but none of the sites are within the geographic area contemplated by the NRC study.

(ii) Guidance. The contracting officer would normally conclude that award of a contract would not place ABC Corp. in a conflicting role where its judgment might be biased. Section 2052.209-72(c) Work for Others, would preclude ABC Corp. from accepting work which could create a conflict of interest during the term of the NRC contract.

(6)(i) Example. AD Division of ABC Corp., in response to a RFP, submits a proposal to assist the NRC in the safety and environmental review of applications for licenses for the construction, operation, and decommissioning of fuel cycle facilities. ABC Corp. is divided into two separate and distinct divisions, AD and BC. The BC Division performs the same or similar services for industry. The BC Division is currently providing the same or similar services required under the NRC's contract for an applicant or licensee.

(ii) Guidance. An NRC contract for that particular work would not be awarded to the ABC Corp. The AD Division could be placed in a position to pass judgment on work performed by the BC Division, which could bias its work for NRC. Further, the Conflict of Interest provisions apply to ABC Corp. and not to separate or distinct divisions within the company. If no reasonable alternative exists, a waiver of the policy could be sought in accordance with §2009.570-9.

(7)(i) Example. The ABC Corp. completes an analysis for NRC of steam generator tube leaks at one of a utility's six sites. Three months later, ABC Corp. is asked by this utility to perform the same analysis at another of its sites.

(ii) Guidance. Section 2052.290-72(c)(3) would prohibit the contractor from beginning this work for the utility until one year after completion of the NRC work at the first site.

(8)(i) Example. ABC Corp. is assisting NRC in a major on-site analysis of a utility's redesign of the common areas between its twin reactors. The contract is for two years with an estimated value of $5 million. Near the completion of the NRC work, ABC Corp. requests authority to solicit for a $100K contract with the same utility to transport spent fuel to a disposal site. ABC Corp. is performing no other work for the utility.

(ii) Guidance. The Contracting Officer would allow the contractor to proceed with the solicitation because it is not in the same technical area as the NRC work; and the potential for technical bias by the contractor because of financial ties to the utility is slight due to the relative value of the two contracts.

(9)(i) Example. The ABC Corp. is constructing a turbine building and installing new turbines at a reactor site. The contract with the utility is for five years and has a total value of $100 million. ABC Corp. has responded to an NRC Request For Proposal requiring the contractor to participate in a major team inspection unrelated to the turbine work at the same site. The estimated value of the contract is $75K.

(ii) Guidance. An NRC contract would not normally be awarded to ABC Corp. because these factors create the potential for financial loyalty to the utility that may bias the technical judgment of the contractor.

(d) Other considerations.

(1) The fact that the NRC can identify and later avoid, eliminate, or neutralize any potential organizational conflicts arising from the performance of a contract is not relevant to a determination of the existence of conflicts prior to the award of a contract.

(2) It is not relevant that the contractor has the professional reputation of being able to resist temptations which arise from organizational conflicts of interest, or that a follow-on procurement is not involved, or that a contract is awarded on a competitive or a sole source basis.

§2009.570-4 Representation.

(a) The following procedures are designed to assist the NRC contracting officer in determining whether situations or relationships exist which may constitute organizational conflicts of interest with respect to a particular offeror or contractor. The procedures apply to small purchases meeting the criteria stated in the following paragraph (b) of this section.

(b) The organizational conflicts of interest representation provision at §2052.209-71 must be included in solicitations and contracts resulting from unsolicited proposals. The contracting officer must also include this provision for task orders and contract modifications for new work for:

(1) Evaluation services or activities;

(2) Technical consulting and management support services;

(3) Research; and

(4) Other contractual situations where special organizational conflicts of interest provisions are noted in the solicitation and would be included in the resulting contract. This representation requirement also applies to all modifications for additional effort under the contract except those issued under the "Changes" clause. Where, however, a statement of the type required by the organizational conflicts of interest representation provisions has previously been submitted with regard to the contract being modified, only an updating of the statement is required.

(c) The offeror may, because of actual or potential organizational conflicts of interest, propose to exclude specific kinds of work contained in a RFP unless the RFP specifically prohibits the exclusion. Any such proposed exclusion by an offeror will be considered by the NRC in the evaluation of proposals. If the NRC considers the proposed excluded work to be an essential or integral part of the required work and its exclusion would be to the detriment of the competitive posture of the other offerors, the NRC shall reject the proposal as unacceptable.

(d) The offeror's failure to execute the representation required by paragraph (b) of this section with respect to an invitation for bids is considered to be a minor informality. The offeror will be permitted to correct the omission.

§2009.570-5 Contract clauses.

(a) General contract clause. All contracts and simplified acquisitions of the types set forth in §2009.570-4(b) must include the clause entitled, "Contractor Organizational Conflicts of Interest," set forth in §2052.209-72.

(b) Other special contract clauses. If it is determined from the nature of the proposed contract that an organizational conflict of interest exists, the contracting officer may determine that the conflict can be avoided, or, after obtaining a waiver in accordance with §2009.570-9, neutralized through the use of an appropriate special contract clause. If appropriate, the offeror may negotiate the terms and conditions of these clauses, including the extent and time period of any restriction. These clauses include but are not limited to:

(1) Hardware exclusion clauses which prohibit the acceptance of production contracts following a related non-production contract previously performed by the contractor;

(2) Software exclusion clauses;

(3) Clauses which require the contractor (and certain of its key personnel) to avoid certain organizational conflicts of interest; and

(4) Clauses which provide for protection of confidential data and guard against its unauthorized use.

§2009.570-6 Evaluation, findings, and contract award.

The contracting officer shall evaluate all relevant facts submitted by an offeror and other relevant information. After evaluating this information against the criteria of §2009.570-3, the contracting officer shall make a finding of whether organizational conflicts of interest exist with respect to a particular offeror. If it has been determined that real or potential conflicts of interest exist, the contracting officer shall:

(a) Disqualify the offeror from award;

(b) Avoid or eliminate such conflicts by appropriate measures; or

(c) Award the contract under the waiver provision of §2009.570-9.

§2009.570-7 Conflicts identified after award.

If potential organizational conflicts of interest are identified after award with respect to a particular contractor and the contracting officer determines that conflicts do exist and that it would not be in the best interest of the Government to terminate the contract, as provided in the clauses required by §2009.570-5, the contracting officer shall take every reasonable action to avoid, eliminate, or, after obtaining a waiver in accordance with §2009.570-9, neutralize the effects of the identified conflict.

§2009.570-8 Subcontracts.

The contracting officer shall require offerors and contractors to submit a representation statement from all subcontractors (other than a supply subcontractor) and consultants performing services in excess of $10,000 in accordance with §2009.570-4(b). The contracting officer shall require the contractor to include contract clauses in accordance with §2009.570-5 in consultant agreements or subcontracts involving performance of work under a prime contract.

§2009.570-9 Waiver.

(a) The contracting officer determines the need to seek a waiver for specific contract awards with the advice and concurrence of the program office director and legal counsel. Upon the recommendation of the Senior Procurement Executive, and after consultation with legal counsel, the Executive Director for Operations may waive the policy in specific cases if he determines that it is in the best interest of the United States to do so.

(b) Waiver action is strictly limited to those situations in which:

(1) The work to be performed under contract is vital to the NRC program;

(2) The work cannot be satisfactorily performed except by a contractor whose interests give rise to a question of conflict of interest.

(3) Contractual and/or technical review and surveillance methods can be employed by the NRC to neutralize the conflict.

(c) The justification and approval documents for any waivers must be placed in the NRC Public Document Room.

§2009.570-10 Remedies.

In addition to other remedies permitted by law or contract for a breach of the restrictions in this subpart or for any intentional misrepresentation or intentional nondisclosure of any relevant interest required to be provided for this section, the NRC may debar the contractor from subsequent NRC contracts.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Information Technology Infrastructure and Support Services

Statement of Work

Table of Contents

C. DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK 1
C.1 OVERVIEW 1
C.2 INTRODUCTION 1
C.3 STATEMENT OF INTENT 2
C.3.1 Core Services and Optional Services 2
C.3.2 Intent for Mutual Cooperation between Offeror and NRC Staff 3
C.3.3 Program Objectives 4
C.3.4 Specific Service Objectives 4
C.3.5 NRC Reserved Rights 5
C.3.6 Additional Contextual Reading 6
C.4 NRC ENVIRONMENT 7
C.4.1 Staff Levels 7
C.4.2 NRC Locations 7
C.4.3 NRC Business Hours 9
C.4.4 Existing Information Technology Infrastructure 9
C.4.4.1 Personal Computing Environment (Desktop/Laptop Computers) 10
C.4.4.1.1 Hardware 10
C.4.4.1.2 Software 10
C.4.4.2 General Server Environment 12
C.4.4.2.1 Hardware 12
C.4.4.2.2 Software 12
C.4.4.3 Application Hosting Server Environment (Optional Task) 13
C.4.4.3.1 Hardware 13
C.4.4.3.2 Software 13
C.4.4.4 Network Appliance, Printers, and Other Hardware 13
C.4.4.5 Incumbent Contractor Staff Levels 15
C.5 CORE SERVICES 16
C.5.1 Basic Infrastructure Support Services 16
C.5.1.1 BlackBerry 16
C.5.1.2 Electronic Mail (Email) and Messaging 18
C.5.1.3 File and Print 20
C.5.1.3.1 File Management 20
C.5.1.3.2 Print Management 21
C.5.1.3.3 Network Attached Devices Management 22
C.5.1.4 Personal Computing and Related Software Licensing 22
C.5.1.4.1 Personal Computing 22
C.5.1.4.2 Office Productivity Software Deployment 25
C.5.1.4.3 Software License Management 25
C.5.1.4.4 Personal Computer Risk Management 26
C.5.1.5 Network Components 26

C.5.1.5.1 Network Management 27
C.5.1.5.2 Wireless Networking 28
C.5.1.5.3 Network Asset Management 28
C.5.1.5.4 Network Device System Administration 28
C.5.1.5.5 Maintenance and Patching Management 29
C.5.1.5.6 Network Monitoring 29
C.5.1.6 Remote Access 31
C.5.1.7 Integration 31
C.5.1.7.1 Project Management 31
C.5.1.7.2 Research 32
C.5.1.7.3 Development 33
C.5.1.7.4 Implementation 35
C.5.1.7.5 Test 35
C.5.1.8 High Performance Computing 36
C.5.2 Service Delivery and Management Responsibilities 37
C.5.2.1 Service Strategy 38
C.5.2.1.1 Strategy Generation 38
C.5.2.1.2 Financial Management 38
C.5.2.1.3 Service Portfolio Management 38
C.5.2.1.4 Demand Management 39
C.5.2.2 Service Design 39
C.5.2.2.1 Service Catalog Management 39
C.5.2.2.2 Service Level Management 40
C.5.2.2.3 Capacity Management 40
C.5.2.2.4 Availability Management 40
C.5.2.2.5 IT Service Continuity (and Backup and Recovery) 42
C.5.2.2.6 Information Security Management 44
C.5.2.2.7 Supplier Management 57
C.5.2.3 Service Transition 57
C.5.2.3.1 Transition Planning and Support 57
C.5.2.3.2 Change Management 58
C.5.2.3.3 Service Asset and Configuration Management 58
C.5.2.3.4 Release and Deployment Management 60
C.5.2.3.5 Knowledge Management 60
C.5.2.4 Service Operation 61
C.5.2.4.1 The Service Desk Function 61
C.5.2.4.2 Event Management 64
C.5.2.4.3 Incident Management 64
C.5.2.4.4 Problem Management 68
C.5.2.4.5 Request Fulfillment 68
C.5.2.4.6 Access Management (and the Directory) 68
C.5.2.4.7 Other Service Operation Considerations 70
C.5.2.5 Continual Service Improvement (CSI) 70
C.5.2.5.1 Centralized Reporting 71
C.5.2.5.2 Proactive Reporting 71
C.5.2.5.3 General Reporting 71

C.6 OPTIONAL SERVICES 73
C.6.1 Computer Facilities Management 73
C.6.1.1 Program Management 73
C.6.1.2 Monitoring 73
C.6.1.3 Quality Assurance 73
C.6.1.4 Backup and Recovery 74
C.6.1.5 Computer Operations 74
C.6.1.6 Physical Facility 75
C.6.1.7 Specialized Systems 75
C.6.1.7.1 Agency-wide Documents Access Management System (ADAMS) 75
C.6.1.7.2 Human Resource Management System 76
C.6.2 Operations Center Network Management 77
C.6.2.1 Operations 77
C.6.2.2 Hardware Maintenance 78
C.6.2.3 Software Maintenance 79
C.6.2.4 Reporting 79
C.6.3 Data Center System Administration 79
C.6.3.1 Project Management 79
C.6.3.2 ADAMS and HLW Meta Systems 80
C.6.3.2.1 Document Storage Support 80
C.6.3.2.2 Database Support 80
C.6.3.2.3 Backup and Recovery 81
C.6.3.2.4 Security Administration 81
C.6.3.2.5 Disaster Recovery 81
C.6.3.2.6 Performance and System Monitoring 81
C.6.3.2.7 Systems Administration 82
C.6.3.3 Mainframe Administration 83
C.6.3.3.1 Application Support 83
C.6.3.3.2 Systems Administration 84
C.6.3.3.3 Backup and Recovery 84
C.6.3.3.4 Training 85
C.6.3.4 HRMS 85
C.6.3.4.1 PeopleSoft Application support 85
C.6.3.4.2 Database Support 85
C.6.3.4.3 Disaster Recovery 86
C.6.3.4.4 Performance System Monitoring 86
C.6.3.4.5 System Administration 86
C.6.3.5 Production Database Management 87
C.6.3.5.1 Application patching 87
C.6.3.5.2 Production Scripts 87
C.6.3.5.3 Disk Space allocation 88
C.6.3.5.4 Database Design 88
C.6.3.5.5 Backup and Recovery 88
C.6.3.5.6 Troubleshooting 88
C.6.3.5.7 Documentation 88
C.6.3.6 NRC Web Servers and Three Tier Environments 89
C.6.3.6.1 Web Server Support for iPlanet and Coldfusion 89

C.6.3.6.2 Performance and System Monitoring 89
C.6.3.6.3 Backup and Recovery 89
C.6.3.6.4 System Administration 89
C.6.4 Wireless Communications Services 90
C.6.4.1 Telecommunications Management and Oversight 90
C.6.4.2 Project Status Reports 91
C.6.4.2.1 Monthly Status Reports 91
C.6.4.2.2 Weekly Status Reports 92
C.6.4.3 Telecommunications Support Services 93
C.6.4.3.1 Maintenance of Property Management Records 93
C.6.4.3.2 Wireless Hardware and services 93
C.6.4.3.3 Products and Services 93
C.6.4.4 Telecommunications Expense Management Services 94
C.6.5 Software License Management 96
C.6.5.1 Software Inventory 96
C.6.5.2 Planning and Design 96
C.6.5.3 Software License Management Tool 97
C.6.5.4 Enterprise License Vendor Management 97
C.6.5.5 Software Catalog 97
C.6.5.6 Usage Reporting and Auditing 97
C.6.6 Safeguards Local Area Network and Electronic Safe Services 98
C.6.6.1 General 98
C.6.6.2 System Administration 99
C.6.6.2.1 Performance Monitoring 99
C.6.6.2.2 Backup 100
C.6.6.2.3 Recovery 100
C.6.6.2.4 Image Backup 100
C.6.6.2.5 Database Administration 101
C.6.6.3 User Support 101
C.6.6.3.1 Access 101
C.6.6.3.2 Helpdesk Support 101
C.6.6.4 System maintenance 102
C.6.6.4.1 Daily 103
C.6.6.4.2 Weekly 103
C.6.6.4.3 Monthly 104
C.6.6.5 Server Shutdown/Restart 104
C.6.6.6 Disaster Recovery 104
C.6.6.7 Configuration Management 105
C.6.6.8 System Documentation Reference Update 105
C.6.6.9 Status Meetings 106
C.6.7 Technology Assessment Center 107
C.6.8 Emergency Response Data System (ERDS) Operations and Maintenance 112
C.6.8.1 General 112
C.6.8.2 Monitoring 113
C.6.8.3 Maintenance 116
C.6.8.4 Management 118
C.6.8.5 ERDS Phase II Support 119

C.6.8.6 Reporting 120
C.6.8.7 Training 120
C.6.9 Secure LAN and Electronic Safe 121
C.6.9.1 General 121
C.6.9.2 User Support 122
C.6.9.2.1 Access 122
C.6.9.2.2 Helpdesk Support 122
C.6.9.3 Records/Document Management 122
C.6.10 Development Facility 123
C.6.11 Microsoft SharePoint Support 124
C.6.11.1 Deliverables 125
C.6.11.2 Ad-Hoc Meetings 126
C.6.12 Extraordinary Move Support 126
C.7 TRANSITION CONSIDERATIONS 127
C.7.1 Initial Transition 127
C.7.2 Other Transition Considerations 128
C.7.3 Transfer of End User Assets to a Successor Offeror or the Government 128
C.8 KEY PERSONNEL 129
C.8.1 Core Services 129
C.8.2 Optional Services 129
C.9 WORKING ONSITE AT NRC FACILITIES 131
Appendix A: Quality Assurance Surveillance Plan (QASP) 134
A.1. Introduction 134
A.2. Surveillance 134
A.3. Unacceptable performance 135
A.4. Service Level Requirements 136
Appendix B: NRC WAN Connections 191
Appendix C: NRC WAN Utilization 192
Appendix D: Space Currently Used by Incumbent Contractors 195
Appendix E: Reporting Requirements 196
Appendix F: Acronyms 210
Appendix G: NRC IT Roadmap 215

C. DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 OVERVIEW

The U.S. Nuclear Regulatory Commission (NRC) is seeking an offeror that has proven experience in developing and maintaining a comprehensive Configuration Management (CM) strategy to provide ongoing agency-wide information technology infrastructure and support services. The new contract is expected to provide the wide range of IT infrastructure services that are included in the current NRC Infrastructure Services and Support Contract (ISSC) (see Section C.5.1 *Basic Infrastructure Support Services*), and also those services currently provided by the NRC wireless telecommunications contract, data center contracts, programmatic IT infrastructure contracts, and additional services to meet the evolving business requirements of the agency.

C.2 INTRODUCTION

The NRC was created as an independent Agency by Congress in 1974 to enable the nation to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. It regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements. The NRC's headquarters are in Rockville, Maryland, and it has a number of other offices around the United States. The NRC currently uses a U.S. General Services Administration (GSA) Seat Management services contract task order to provide agency-wide Information Technology (IT) infrastructure and support services. The final option year for the order ends on September 27, 2010 (with the potential of being extended until December 27, 2010).

C.3 STATEMENT OF INTENT

It is the intention of the NRC to award this contract, in its entirety, to a single prime vendor. This prime vendor will be responsible for the management of all deliverables under the contract.

The period of performance for the new ITISS contract is expected to be:

Base Period:	February 18, 2011 – February 17, 2014
Option Year 1:	February 18, 2014 – February 17, 2015
Option Year 2:	February 18, 2015 – February 17, 2016
Option Year 3:	February 18, 2016 – February 17, 2017

C.3.1 Core Services and Optional Services

This Statement of Work (SOW) includes descriptions of core services and optional services. The NRC's infrastructure is currently managed under a series of contracts. The first of these, the ISSC, is primarily used for seat management, some server support for shared administrative applications, and IT infrastructure research, development, and testing. Other contracts currently providing ITISS services which are also described in this Statement of Work can be found in Table 1, below.

Contract Description	Start	Base End	Options
Data Center Facilities Operations;	FY 2009 Q3	FY 2012 Q3	2 (1 Year Each)
Data Center System Administration;	FY 2010 Q2	FY 2011 Q2	4 (1 Year Each)
Wireless Telephone Services Management;	FY 2009 Q3	FY 2010 Q3	4 (1 Year Each)
Nuclear Security and Incident Response (NSIR) Operations Center Network Management.	FY 2010 Q1	FY 2011 Q1	4 (1 Year Each)
Safeguards Wireless Local Area Network	FY 2009 Q1	FY 2018 Q4	10 (1 Year Each)
Emergency Response Data System	FY 2011 Q1	FY 2012 Q1	4 (1 Year Each)

Table 1 - Current Contracts providing ITISS Services at the NRC

It is the intention of the NRC to consolidate all of these services into the Information Technology Infrastructure and Support Services (ITISS) contract. Some of the optional tasks describe activities that are not currently being performed at the NRC. It is the NRC's

expectation that some optional tasks will be awarded within months of initial contract award. Assuming the offeror demonstrates a high-level of performance in delivering the core tasks and initial optional tasks, the NRC intends to award the remaining optional tasks at the earliest expiration of the base or option year for an existing contract.

Offerors intending to propose solutions that will be hosted external to NRC-owned facilities for either core or optional services must clearly demonstrate that they have experience providing such solutions adhering to all of the security and performance requirements of the Federal Government and the NRC.

In order to provide an accurate account regarding the current state at the NRC, the SOW provides significant detail on current inventory and corresponding management practices. While this level of detail may appear to dictate specific technologies or solutions in many places, the NRC is very open to the proposal of innovative technologies and/or solutions that would provide greater efficiencies (including "green improvements" which would decrease the environmental impact of NRC work practices) and/or better service. In proposing innovative improvements, the NRC is also interested in timeframes and roadmaps to migrate from "as is" to the proposed "to be." The NRC is not flexible about IT security requirements or performance requirements; all innovative proposals must adhere to security and performance requirements of the Federal Government and the NRC.

The offeror shall provide hardware and software used by the offeror in the performance of work under this contract (e.g. personal computers for the offeror's staff, network management software tools, etc.) and incorporated into the price for the proposed services.

The NRC also expects the offeror to comply with all requirements set forth in NRC Management Directives (MD) (see http://www.nrc.gov/reading-rm/doc-collections/management-directives). MDs may be periodically updated during the course of this contract, and the offeror shall comply with updated versions. It is also expected that prospective vendors consider the agency's goals and objectives, which include identifying and implementing green improvements, when planning for innovative solutions.

C.3.2 Intent for Mutual Cooperation between Offeror and NRC Staff

The NRC wishes for the chosen offeror to mutually cooperate with NRC staff. Such cooperation would meet the needs and desires of both the offeror and the NRC in a cost-effective way. For example:

1. The NRC desires an offeror that will leverage technology in their proposal to provide excellent service at a reasonable cost to both the offeror and to the NRC;
2. Throughout the course of the contract, the NRC intends to actively solicit suggested changes in behaviors or the environment that will result in cost savings that can be reinvested in improved service or additional services;
3. The NRC is interested in continual improvement of service delivery using an Information Technology Infrastructure Library version 3 (ITIL v3)-based service delivery model. The offeror shall provide service delivery using appropriate ITIL v3 best practices and assist the NRC in maturing its overall service delivery;
4. Within this document, occasional reference is made to the offeror providing their "best effort" to accomplish a service that is difficult to predict (e.g. support of printers

that are not owned by the offeror, but rather are owned by the NRC). For the purposes of this document, "best effort" will include such activities as:

- Installation of software/hardware/drivers
- Testing to verify software/hardware works
- Limited troubleshooting

When problems are identified, a "best effort" service support would include using the following resources to try and resolve the problem:

- Internal resources – technicians, developers
- Internet
- Manufacturer Support
- Attempt work around

If none of these attempts are successful, the problem shall be returned to the NRC for resolution. The offeror shall not apply Service Level Requirements (SLRs) to "best effort" service provisioning, other than to issue a ticket that will be logged into the service desk system for the Agency's use in tracking whether or not the problem has been resolved. Open "best effort" tickets are not to be included in calculating any performance-based SLRs.

All offerors will be required to provide references on their past performance with previous clients.

C.3.3 Program Objectives

The NRC intends to establish a performance based contract to provide the full scope of IT infrastructure support to its customers. The programmatic objectives for this acquisition include:

1. Consistent provision of IT infrastructure support services at the required levels of service for the most reasonable cost;
2. Maintaining a robust, secure computing environment that protects the information and users that the IT infrastructure supports;
3. Adaptability of the IT infrastructure to changes in requirements and priorities;
4. Creation and promotion of collaboration between the NRC staff and the offeror to support all services under this contract; and,
5. Innovation in the use of information technology to increase the productivity of agency users, improve the agency's security posture, and reduce the cost of services provided while maintaining customer service expectations

C.3.4 Specific Service Objectives

Through this acquisition, the objectives of the NRC are to:

1. Allow NRC staff to effectively work securely from anywhere at any time;
2. Provide a highly consistent user support environment that meets or exceeds agreed upon performance standards;
3. Establish and maintain an effective security posture for NRC information and information systems to reasonably prevent the compromise of NRC resources that are interconnected with the NRC network and complies with appropriate Federal and agency policy and regulations;
4. Establish and maintain a rigorous framework for the management of Information Technology Infrastructure (ITI) services (i.e. ITIL version 3 (ITIL v3), ISO 20000);
5. Provide centralized support for agency users that they can obtain at any time from anywhere through a variety of mechanisms;
6. Proactively review ITI incidents to recognize patterns, establish baselines, implement improvements, provide training and solve problems to improve users' experiences;
7. Proactively monitor the infrastructure and implement mitigations for recognized problems and issues;
8. Plan for and ensure that disruptions to ITI resources have a minimal downtime and impact on NRC users;
9. Understand business requirements of Agency users and how they impact the services within the ITI to enhance its effectiveness in support of the NRC mission;
10. Manage provisioned and Government furnished ITI related assets and the configuration of those assets to ensure an accurate, reliable, and complete inventory;
11. Establish an effective quality assurance program that ensures continuous improvement in support of the business needs of the NRC users;
12. Leverage technology to increase availability of critical business services as well as remote access; and
13. Participate in the creation and maintenance of local operating and quality assurance procedures and establish and maintain a virtual library for all documentation available through the NRC Intranet.

C.3.5 NRC Reserved Rights

The NRC reserves the right to make final decisions on all solutions proposed by the vendor and to inspect any part of the ITI at any time. There shall be no components of the NRC environment that are not accessible to designated NRC employees without having to request access. Specifically:

1. NRC will perform periodic reviews to ensure that the systems produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event and the identify of any user/subject associated with the event;

2. NRC will have unrestricted access to IT system audit tools and generated audit log information; and,
3. NRC will monitor and independently validate the implementation of NIST 800-53 security controls.

NRC will be able to monitor data flow and will be able to investigate through the use of NRC approved tools any instance or areas where suspicious or abnormal activity occurs.

C.3.6 Additional Contextual Reading

The following links provide reading that may aid prospective offerors in better understanding the NRC's goals and history:

1. NRC Strategic Plan: Part *V. Management, Strategies and Means to Support Management Strategies, D. Expanded Electronic Government*

   http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1614/v3/

2. NRC Information Technology/Information Management (IT/IM) Strategic Plan

   http://adamswebsearch.nrc.gov/idmws/ViewDocByAccession.asp?AccessionNumber=ML081150680

3. NRC – Office of Management and Budget Exhibit 300s: *Infrastructure Services and Support*

   http://www.nrc.gov/reading-rm/doc-collections/omb-exhibit-300s/

4. NRC History

   http://www.nrc.gov/about-nrc/history.html

C.4 NRC ENVIRONMENT

This section provides detailed information on the current environment, the existing hardware/software infrastructure, and the expected ITI user levels at the NRC. The staff levels are approximate and may vary over time. The environment and software/hardware infrastructure are provided as guidelines to assist in creating an appropriate proposal. For example, there is little server virtualization currently, but virtualization may be an appropriate suggestion to make in proposals if the vendor can provide increased efficiency, reduced cost, and adequate security.

C.4.1 Staff Levels

The current NRC level of 5,500 personal computer users (including both NRC employees and NRC contractors) is expected to grow at a rate of 3% per annum. This growth is not guaranteed but should be incorporated for planning purposes.

C.4.2 NRC Locations

Information on the NRC locations can be found on the website at http://www.nrc.gov/about-nrc/locations.html. The NRC has its Headquarters in Rockville, Maryland, and a number of other offices around the United States.

- The six-building headquarters complex (http://www.nrc.gov/about-nrc/locations/hq.html) in Bethesda and Rockville, Maryland, houses our headquarters staff and our Public Document Room (http://www.nrc.gov/reading-rm/pdr.html). There are approximately 4000 ITI users at these locations.

  During the ITISS period of performance, four of these buildings will be consolidated to a single new building that will be constructed (See paragraph below and section C.6.12 Extraordinary Move Support). The offeror shall provide the services described in this SOW both in the current headquarters buildings and the future headquarters building. It is expected that there will be some reduction in cost for some services once those buildings have been consolidated into a single building adjacent to the White Flint headquarters complex.

- The Region I Office (http://www.nrc.gov/about-nrc/locations/region1.html) in King of Prussia, Pennsylvania, oversees our regulatory activities in the northeastern United States. There are approximately 211 ITI users at this location.

- The Region II Office (http://www.nrc.gov/about-nrc/locations/region2.html) in Atlanta, Georgia, oversees our regulatory activities in the southeastern United States. There are approximately 175 ITI users at this location.

- The Region III Office (http://www.nrc.gov/about-nrc/locations/region3.html) in Lisle, Illinois, oversees our regulatory activities in the northern midwestern United States. There are approximately 189 ITI users at this location.

- The Region IV Office (http://www.nrc.gov/about-nrc/locations/region4.html) in Arlington, Texas, oversees our regulatory activities in the western and southern mid-western United States. There are approximately 160 ITI users at this location.

- The On-Site Representative High-Level Waste Management Office (http://www.nrc.gov/about-nrc/locations/hlw-office.html) in Las Vegas, Nevada, maintains information associated with the proposed high-level waste repository (http://www.nrc.gov/waste/hlw-disposal/reg-initiatives/review-site-

recommend.html).There are approximately 20 personal computers supported at this location.

- The NRC Technical Training Center (http://www.nrc.gov/about-nrc/locations/training.html) in Chattanooga, Tennessee, provides training for the staff in various technical disciplines associated with the regulation of nuclear materials and facilities. There are approximately 28 ITI users at this location.
- The NRC also has onsite inspectors permanently stationed at each reactor licensee that it regulates (http://www.nrc.gov/info-finder/reactor/). These Resident Inspectors require broadband access to the NRC network and use applications that are hosted at NRC Headquarters, the Regional Offices, and on the internet. There are currently over 100 locations that must be supported.
- The NRC ITI is extended to an application support facility. This facility is provided by an application development support contractor. The work performed under that contract is outside the scope of ITISS. The application support contractor supplies the Wide Area Network (WAN) connection from this facility to NRC Headquarters and provides the network router at the application facility end of that connection. The application support contractor manages that router. A domain controller and personal computers shall be supplied by the ITISS offeror. In addition, the ITISS offeror shall supply help desk support, desk-side support, and network monitoring for the equipment provided and the network at the application support facility. There are approximately 75 ITI users at this location.

From Fiscal Years (FY) 2013 – 2015, the NRC will centralize all headquarters staff not currently located in One White Flint North or Two White Flint North into a new building in Rockville, Maryland. The NRC anticipates 1500 staff moves in FY 2013, and 6000 extra staff moves in each of FY 2014 and FY 2015 to achieve consolidation (some people will be moved more than once). These moves are in addition to the current average annual moves of 1000. Appendix C provides square footage and descriptions of the space that will be available to the ITISS offeror's staff.

While the primary computing and support facilities are located at the Headquarters campus, each regional office also maintains local computing and support capabilities, including some local email functions (Exchange satellite servers) which are provided by the incumbent ISSC contractor. The offeror shall provide dedicated system administration support at the Regional Offices to maintain network components and servers. The offeror's staff will be primarily responsible for the management of the Regional Local Area Networks (LANs) and Wide Area Network (WAN) interfaces. In addition, they will provide Tier 2 Help Desk support as well as desk-side support as requested by a Regional Contracting Officer Technical Representative (COTR). Currently, user support is primarily provided by NRC Regional staff or non ITISS contractors.

During the ITISS period of performance, there will be additional remote sites that will be added to the ITI due to the construction of new nuclear power facilities. The offeror shall provide network devices (local router, etc.), personal computer equipment for the site, and network management for that segment of the network as if it were a Resident Inspector site. It is unknown precisely when each new power plant will be constructed, but there is information available about the locations of the proposed sites (http://www.nrc.gov/reactors/new-reactors/col/new-reactor-map.html) and the current licensing schedule (http://www.nrc.gov/reactors/new-reactors/new-licensing-files/new-rx-

licensing-app-legend.pdf). However, only the licensee will determine if and when construction will begin.

C.4.3 NRC Business Hours

Currently normal working hours are 6am-9pm Eastern Standard Time/Eastern Daylight Time (EST) Monday thru Friday excluding Federal Holidays. Maintenance and production changes typically shall not be made during normal working hours. However, it should be noted that new organizational changes allow users to report to work as early as 5am. As such, through results from trending and analysis, it may be necessary to adjust these hours either way throughout the life of the contract.

Some specific functions require 24 x 7 x 365 support – these are noted within the SOW.

C.4.4 Existing Information Technology Infrastructure

The following diagram provides an overview of the existing technology infrastructure for the Core functionality and the two Data Center optional tasks. All information provided in this section of the document is intended for informational purposes only and should not be construed to dictate preference.

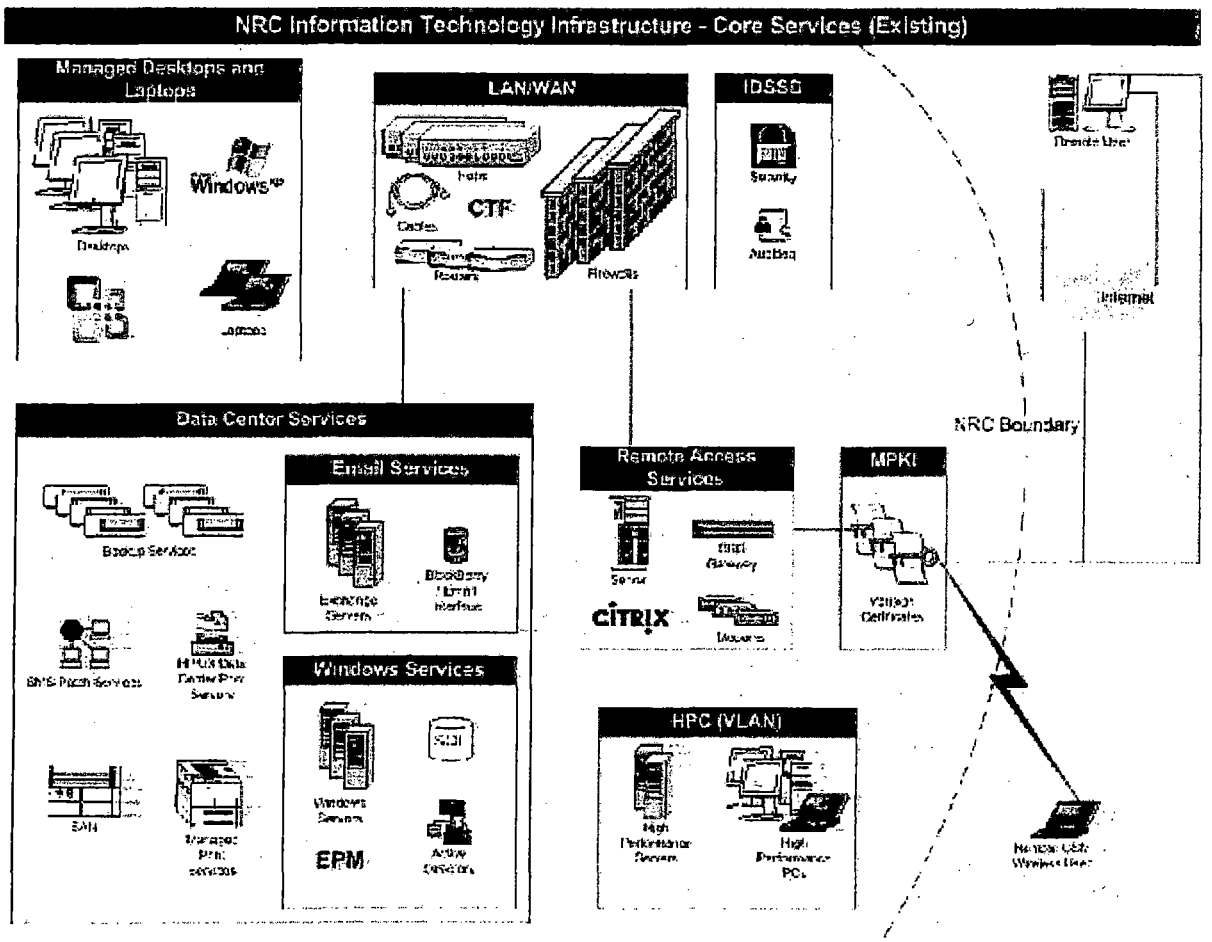

Figure 1 - NRC Information Technology Infrastructure – Core Services

C.4.4.1 Personal Computing Environment (Desktop/Laptop Computers)

C.4.4.1.1 Hardware

For the current base of approximately 5,500 personal computer users the NRC currently has:

- 5,450 desktop computers furnished by the incumbent ISSC contractor;
- 310 laptop computers that are managed under the current IT infrastructure and furnished by the incumbent ISSC contractor;
- Approximately 1000 Government-furnished laptop computers that are not managed by the current incumbent ISSC contractor. These Government Furnished Equipment (GFE) laptop computers are in the process of moving from non-managed to managed under the current ITI contract; and,
- 100 High-performance computing workstations furnished by the Government.

All computers provided under the current contract are supported on a 3-year refresh cycle. These personal computers are distributed in approximate proportion to the number of NRC staff located in our Regional Offices and satellite offices as outlined in section *C.4.2 NRC Locations*.

C.4.4.1.2 Software

The following (Table 2) are a sample of the typical software found on current NRC personal computers (PCs) (Desktops/Laptops). In some cases a mix of previous generation products and newer generation products exist (e.g. Microsoft Office). Under the new contract the NRC expects to license current generation products. Note, the Agency-wide Documents Access and Management System (ADAMS) is a Government-owned system. ADAMS is a document management system written in Visual Basic, based on IBM FileNet and includes a client-based software component.

Workstation Component	Current Version	Source
ADAMS Desktop (NRC Custom)	4.8	NRC Supplied
ADAMS for MSOffice (NRC Custom)	1	NRC Supplied
ADAMSOutlookIntegration (NRC Custom)	1.1	NRC Supplied
Adobe Acrobat Reader	8	Incumbent Supplied
Adobe Flash Player	10.0	Incumbent Supplied
Adobe SVG Viewer	3	Incumbent Supplied
Apple QuickTime	7.6	Incumbent Supplied
Autodesk Design Review 2008	4.1	Incumbent Supplied
Delphi NRC Telephone Directory	1.0	NRC Supplied
Diskeeper Professional Edition	8.0	Incumbent Supplied
FileNet Content Services Client Libraries	5.4	NRC Supplied
FileNet IDMDT	3.2	NRC Supplied
FileNET Panagon IDM Desktop	3.2	NRC Supplied
FTI Microshield	5	NRC Supplied
FTP Software OnNet32	3	Unsupported

Workstation Component	Current Version	Source
HRMS (NRC Custom)	1	NRC Supplied
Inso Outside-In Viewer (ADAMS component)	8.0	NRC Supplied
Metastorm Informs Filler	4.3	NRC Supplied
Microsoft .NET Framework	1.1	Incumbent Supplied
Microsoft .NET Framework	2.1	Incumbent Supplied
Microsoft .NET Framework	3.5	Incumbent Supplied
Microsoft Collaboration Data Objects	6.5	Incumbent Supplied
Microsoft Data Access Objects (DAO)	3.5	Incumbent Supplied
Microsoft Internet Explorer	6.0	Incumbent Supplied
Microsoft MDAC	2.8	Incumbent Supplied
Microsoft Office Professional Edition 2003	11.0	Incumbent Supplied
Microsoft Office Visio Viewer 2003	11.0	Incumbent Supplied
Microsoft Outlook 2007	12.0	Incumbent Supplied
Microsoft Windows Genuine Advantage	1.3	Incumbent Supplied
Microsoft Windows Installer	3.1	Incumbent Supplied
Microsoft Windows Media Player	11.0	Incumbent Supplied
Microsoft XML	4.0	Incumbent Supplied
PkWare SecureZip	8.2	Incumbent Supplied
PowerBuilder	8.0	NRC Supplied
Real Player Enterprise Player	2.1	NRC Supplied
SQL Drivers for NT	6.5	NRC Supplied
Sun Java	6.1	Incumbent Supplied
Sybase Adaptive Server Enterprise	12	NRC Supplied
Symantec Antivirus	11.0	Incumbent Supplied
Symantec LiveUpdate	3.1	Incumbent Supplied
Wang Imaging	5.0	Unsupported
Wang Watermark	3.1	Unsupported

Table 2 – Sample of typical personal computing software

Notes:

a) Software maintenance and development on ADAMS are not part of this SOW. Support of the ADAMS server infrastructure is included in the optional tasks for Computer Facilities Management and Data Center Administration. Installation and troubleshooting of the configuration of the client component is part of the core Personal Computing component of this SOW.

b) Any software listed as "unsupported" shall be supported on a best effort basis by the offeror. Best effort is defined in section C.3.2 Intent for Mutual Cooperation between Offeror and NRC Staff.

c) PowerBuilder 8 supports specific legacy applications. This application is not part of the standard image. Support requirements only include installation on an as needed basis and minor troubleshooting.

d) The current operating system (OS) is Windows XP. The NRC has currently elected not to upgrade to Windows Vista, but will upgrade to Windows 7. The NRC shall have the option to upgrade to a new OS within 6 months of release, but may elect not to upgrade if it is deemed unwise.

C.4.4.2 General Server Environment

The NRC general server environment consists of network servers, file servers, and those servers used within the NRC which support the general network environment (shared storage, electronic mail, network management). These servers are primarily owned by the incumbent ISSC contractor.

C.4.4.2.1 Hardware

The NRC general server environment currently consists of one-hundred seventy-five (175) servers. These servers consist of machines with one to four central processing units (CPUs) or in the case of dual-core or quad-core processors, one to four processing cores. None of the current servers utilize more than four CPUs or a total of four processor cores. The majority of servers in the general server environment run Windows; however, some run a Linux kernel. Specifically, the current general server breakdown is as follows:

- Wintel Servers with 1-4 CPUs: One-hundred sixty-five (165) servers; and,
- Unix/Linux Servers with 1-4 CPUs: Ten (10) servers.

The offeror will propose a server refresh cycle. The NRC is flexible, but in general believes no server should be allowed to forego support.

C.4.4.2.2 Software

The following is a sample of the typical software found on current NRC Servers in the general server environment. The environment is evolving, and specific applications may vary at the time of contract award. The intent of this list is to define the general types of software currently in use.

- Active Directory;
- Asset Management System (WiseTrack);
- BlackBerry Enterprise Server;
- CiscoWorks;
- Citrix;
- Finjan;
- Helpdesk Ticketing System (BMC Service Desk);
- IronPort;
- LANDesk Management Suite;
- Microsoft Exchange Enterprise;

- Microsoft Exchange Standard;
- Patchlink;
- Structured Query Lanaguage (SQL) Server 2000/2005;
- Symantec Antivirus;
- Symantec BESR imaging tool;
- System Center Operations Manager;
- Tivoli Storage Manager (TSM) Backup Client;
- BrightStor ArcServ;
- Vulnerability Scanner (NCircle);
- What's Up Professional (monitoring); and,
- ZENworks.

C.4.4.3 Application Hosting Server Environment (Optional Task)

The Application Hosting server environment (also referred to as NRC Data Center Environment) consists of those servers that generally are used for hosting specialized applications. These servers are currently primarily owned by the NRC. The NRC would prefer that all components of the ITI eventually be offeror-supplied as the GFE reaches the end of its useful life.

C.4.4.3.1 Hardware

The NRC Data Center environment currently consists of 323 servers. As with the general server environment hardware described in Section C.4.4.2.1 General Server Environment: Hardware, all of the Data Center servers consist of machines with one to four CPUs or in the case of dual-core or quad-core processors, one to four processing cores.

The agency also takes advantage of processor time on an NIH mainframe server for some of its legacy applications. There are printers located within the NRC that are connected to these NIH systems which the incumbent Data Center Facilities Operations contractor maintains and manages both the printers and the printout sorting. In addition, the incumbent Data Center Facilities Operations contractor occasionally works with NIH personnel and contractors to troubleshoot connection problems as directed by the NRC PM.

C.4.4.3.2 Software

Other than custom software or applications developed specifically for the purpose of meeting NRC requirements, the software expected in the Data Center environment is similar to that described for the general server environment in Section C.4.4.2.2 General Server Environment: Software, with the addition of VMWare.

C.4.4.4 Network Appliance, Printers, and Other Hardware

Appendix A provides a diagram of the basic topology and link speeds of the NRC network. The offeror is not responsible for providing the WAN links, but is responsible for coordinating with the Provider to troubleshoot incidents and determine root cause. The offeror is not responsible for the links between buildings or the cabling plant itself.

In addition to the desktop/laptop, general server, and data center server environments, the NRC has other hardware components and devices that serve as part of the IT Infrastructure. This additional hardware consists of:

- Network appliances including routers, switches, gateways;
- Network security appliances and firewalls;
- Tape back-up devices;
- Redundant Array of Independent Disk (RAID) devices and/or Storage Area Networks (SAN);
- Network Printers (both color and black & white);
- Local printers; and,
- Scanners and plotters.

The following table (Table 3) provides a current list of hardware that falls in this category. It is expected that an ITISS vendor will initially manage this existing hardware and then as required, replace components with suitable current-day replacements. By "current-day" the NRC means current as of the date of replacement.

Hardware Description	Quantity
Cisco 1700 Router	1
Cisco 2800 Router	74
Cisco 3700 Router	33
Cisco 3800 Router	14
Cisco 7200 Router	1
Cisco 2960 Series Switch	15
Cisco 3750 Series Switch	34
Cisco 4500 Series Switch	46
Cisco 6500 Series Switch	8
Host Intrusion Protection System	1
HP 4650 Color Network Printer/+GFE	80/19
HP 4350/HP 4515x B/W Network Printer/+GFE	292/2
HP 9040 B/W Network Printer	38
XIOTech SAN	1
Fibre Switch (Silkworm 4100)	2
Tape Library (Spectra Logic T120Q)	2
Tape Drive (Spectra Logic T50)	7
Firewall (Base)	1
Firewall Proxy/ZONE	14
48 Port 10/100 Ethernet Module	179
48 Port 10/1000 Ethernet Module	25
Local Printers (Various Makes/Models), GFE	2,000
Plotters	10
Multifunction Printers	36
Scanners	211

Table 3 - Network Appliances, Printers, & Other Hardware

C.4.4.5 Incumbent Contractor Staff Levels

Incumbent contractor staff levels are a combination of support for core functions charged as part of the seat management fee and additional contractor or NRC staff members who perform functions such as integration and test. These numbers are approximate and are supplied to inform potential offerors on the general level of effort currently expended; they are not meant to dictate future staffing levels. The estimates are as follows:

20 Integration;

3 Test Facility;

9 Headquarters (HQ) Remote Building Dedicated Sys Administrators;

10 Regional and Technical Training Center Support;

9 Extended Hours Dedicated Support - Help Desk;

8.5 Extended Hours Dedicated Support - Network Operations;

2 Laptop Patching/Maintenance Support/Loaner Laptop Program administration;

1 Technical Writer;

10 Operational IT Security Support;

10 Network Operations;

10 Help Desk - Telephone/Remote Support;

10 Help Desk – Desk-side support;

4 High Performance Computing Support;

5 Management and Administration;

1 Technology Assessment Center;

4 HQ Remote Building Dedicated System Administrators;

5 HQ Remote Building Dedicated Desk-side Support

5 Desktop Refresh

In addition, incumbent contractor staff levels that are currently dedicated to optional tasks are as follows:

6 Computer Facilities Management;

2 Nuclear Security and Incident Response (NSIR) Operations Center Network;

18 Data Center System Administration;

15 Telecommunications;

4 Wireless Communications Services; and,

1 Safeguards Information (SGI) Wireless System Administration Services.

C.5 CORE SERVICES

This section describes services to be provided under the Core ITISS contract. These services consist of basic infrastructure support services (e.g. messaging, file and print) in alphabetical order, followed by a further description of the NRC's and offeror's service delivery and management responsibilities. The responsibilities are structured in terms of the ITIL v3.

It should be noted that the offeror shall include a transition schedule and pricing in the proposal which is described in Section *C.7 Transition Considerations*.

Within this SOW, there is a description of the building space provided by the NRC to the incumbent ISSC contractor's staff (See Appendix D: Space Currently Used by Contractors Performing ITISS Core and Optional Tasks). The offeror shall be responsible for providing staff to address all of the requirements described in this SOW, even if the number of staff required to do that exceeds the office space allocated by the NRC for those offeror staff. The offeror shall include in their proposal how they intend to use NRC provided space as well as how they intend to use any additional office space (provided by the offeror) to fulfill the SOW requirements. The offeror's proposal shall include any connectivity that a facility will require to the NRC ITI, and how it addresses Federal and NRC requirements for physical security, personnel security, and IT security. Any costs associated with an offeror-supplied facility shall be incorporated into the offeror's cost proposal.

C.5.1 Basic Infrastructure Support Services

Each of the following subsections describes a core service to be provided under the base contract. As a general rule, the services in this section are primarily describing "what will be managed." Taken together with the ITIL-based services described in Section C.5.2 Service Delivery and Management Responsibilities, they should be considered the main body of work to be included in the base (non-optional) tasks. Also, the Service Level Requirements found in Appendix A were designed to correlate with technical requirements of the SOW and should be referred to when the offeror is developing its proposal.

C.5.1.1 BlackBerry

The NRC currently furnishes approximately 1000 BlackBerrys. The current device and service providers are Verizon, T-Mobile, and AT&T. Mobile access to email, the Web, and mobile applications has become increasingly important as the mission of the Agency has expanded, the Agency workforce has changed, and flexibility in the workplace has increased. Many Agency users are regularly away from their offices but still have a need to stay connected to their co-workers to meet mission objectives. Other users are required to attend meetings and still respond rapidly to staff decision requests.

Some Agency users frequently travel outside of the country and need to maintain access to the same functionality on their BlackBerry that they have locally. There are other users that only travel oversees occasionally, but require that same continuity of service internationally. Since NRC users are based all over the United States, it is also important that service plans provide availability where the staff member is located.

In addition, the offeror shall:

1. Manage BlackBerry accounts and the interface with corresponding Microsoft (MS) Exchange email accounts according to optimization standards recommended by Research In Motion (RIM) Corporation;

2. Maintain the high-availability BlackBerry infrastructure within the NRC so that a BlackBerry Enterprise Server (BES) failure will not result in loss of availability to BlackBerry users;
3. Monitor BlackBerry infrastructure for any events and manages capacity of the service;
4. Provide all BlackBerry capabilities available by the device and service plan providers that meet Federal IT security policy requirements and NRC-specific security requirements as requested and approved by the NRC;
5. Enforce secure access to BlackBerry devices through a strong device password policy; Remotely erase data contained on BlackBerry devices that have been lost or stolen at the request of the NRC.
6. Minimize the amount of time that a user is without a blackberry unit (due to either provisioning or repair); and,
7. Minimize the length and frequency of service outages.

Currently BlackBerry support is performed under two separate contracts. The desire is to have all BlackBerry support under the ITISS contract; however support under the core services is limited to:

1. BlackBerry Integration with Exchange
2. BlackBerry Enterprise Server(s) (BES) Management: Manage accounts for BlackBerry users and links between e-mail device and BlackBerry devices.
3. BlackBerry Services Monitoring
4. User Support for account issues and minor device issues
5. BlackBerry Policy Management
6. BlackBerry Device Firmware Upgrades and Management
7. BlackBerry Device and Function Testing: Evaluate new BlackBerry devices and/or functions and test them to ensure appropriate security and functionality.

Other BlackBerry support is included in the optional wireless services task in Section *C.6.4 Wireless Communications Services*. The following services are not included in the Core Services and are listed in this section only to provide clarity around BlackBerry support. The services included in the optional task are:

1. Inventory and reconciliation of the wireless inventory of services and hardware in the Office of Information Services (OIS) Infrastructure and Computer Operations Division (ICOD) Computer Operations and Telecommunications Branch (COTB) NRC Space and Property Management System (SPMS) property account and the telecommunications expense management (TEM) tool;
2. Property storage and control of on-hand wireless hardware;
3. Service request processing using both the Government provided service desk ticket request system and the TEM tool to process and fill the appropriate orders to meet the Government's approved requirements;

4. Acquisition of BlackBerry devices;
5. Property distribution/return;
6. BlackBerry server support in the area of assisting the Government in identifying service problems for the end users that may make their appearance known on the server; such as a missing PIN, etc;
7. User device/service training to ensure that the user is familiar with the device they are issued; to allow them to place and receive cellular calls; unlock their BlackBerry, the procedures for charging and caring for the devices, etc;
8. Coordinating with the wireless carriers and the Government customer on the movement of a cellular number from one device to another using the same carrier or between carriers;
9. Pairing Bluetooth hardware (headsets, vehicle mount, vehicle charger, and GPS navigation utility, etc.) with cellular devices when requested; and
10. Preparing cellular phones and BlackBerry devices for issuance in the fulfillment of an authorized work order.

Currently, the NRC is satisfied with BlackBerry devices and the interconnections with the agency's email system. The NRC is open to other mobile computing devices over time (See *C.5.1.4 Personal Computing and Related Software Licensing*). However, the NRC would like to maintain a standard with a manageable set of devices and does not want to incur significant costs or complexity associated with managing too many mobile platforms.

C.5.1.2 Electronic Mail (Email) and Messaging

The NRC currently uses Microsoft Exchange 2007 and Outlook 2007 for delivering its email service. Generally users are allocated one (1) gigabyte (GB) of network storage space for mail. Outlook Web Access is also available for users to access their email remotely. Electronic mail services have been integrated with both NRC customized and commercial off-the-shelf (COTS) software applications (i.e. Microsoft Office, Microsoft SharePoint, ADAMS, etc.) to allow for collaboration and storage of official records.

The offeror shall evaluate the current use of e-mail storage at the NRC and make recommendations about appropriate per user e-mail storage allocations. These recommendations will include definitions of distinct user classes which may have different e-mail storage allocation requirements. The offeror shall also recommend an appropriate incremental increase in e-mail storage allocation per user/per year. The offeror shall provide pricing for this incremental storage.

The offeror shall:

1. Manage, operate, maintain, administer and support NRC email services including internal email as well as Internet email capability;
2. Define and maintain users, distribution groups and system profiles;
3. Develop and maintain workflow definitions for the mail system environment;
4. Monitor mail statistics such as inbound and outbound mail flow;

5. Provide metrics on system-related incidents and events; utilize this data to detect and resolve systemic problems;
6. Monitor email system utilization and disk space usage and enforce Agency email size limitations;
7. Track and remove messages at the request of the NRC operational security staff when classified or Safeguards information spills occur or when data leakage occurs;
8. Review systems logs, email and performance data to ensure optimum system operation;
9. Respond to and resolve all user issues related to internal email services or Internet email service;
10. Provide software updates and security updates for the email desktop client as well as the back-end email applications, following NRC Release and Deployment Management Plans;
11. Perform nightly E-mail back-ups and maintain them in accordance with NRC retention requirements;
12. Monitor electronic mail storage and provide increased capacity (up to 10%) as appropriate on an annual basis;
13. Provide, manage, operate, maintain, administer and support a secure instant messaging (IM) service between users within the NRC ITI (the NRC is currently integrating Microsoft Office Communication Server into its production environment);
14. Provide, manage, operate, maintain, administer and support a unified messaging service that will provide NRC users with a computer-based interface for email, voice mail, PBX, and messaging (the NRC does not currently use unified messaging);
15. Restore email from back-up as requested;
16. Manage replication of e-mail from NRC headquarters data center to a designated disaster recovery site to ensure continuity of e-mail once NRC initiates a Continuity of Operations (COOP) event;
17. Manage the interface between Microsoft (MS) Exchange email accounts and their corresponding BlackBerry accounts according to optimization standards recommended by Microsoft Corporation;
18. Minimize the amount of time that a user is without an e-mail account/client (due to either provisioning or repair);
19. Minimize the length and frequency of service outages;
20. Minimize the time necessary to periodically backup data, and to restore electronic messaging data from backups; and,
21. Minimize the time necessary to provision increased storage capacity when requested.

The offeror shall provide upgrades to Outlook and Exchange (e.g. Exchange 2010) as these products become available and when they are approved by the NRC. The offeror shall ensure that no additional cost is incurred by the NRC for upgrades providing comparable services. When NRC determines that it is appropriate to upgrade to a newer version of the

software, the offeror will manage a complete upgrade of not only the software, but migration of individual user data. As new releases become available, there may also be opportunities for new features to be utilized by the NRC. The offeror shall make recommendations about new feature sets and will work with the NRC to select the best features for the NRC environment. Please see section C.5.1.4.3 Software License Management of this SOW for more information about software license management and upgrades.

The offeror shall provide an e-mail encryption solution for the transmission of electronic mail outside of the Agency. This encryption solution must meet all Federal Government and NRC-specific requirements for security. For externally bound e-mail, the offeror shall provide encryption at the e-mail gateway that will be decrypted at the recipient's desktop. For internal e-mail, the offeror shall provide a solution that will utilize existing VeriSign electronic certificates. The offeror shall also supply a mechanism to ensure non-repudiation of emails sent from or to the NRC.

C.5.1.3 File and Print

C.5.1.3.1 File Management

Information is by far the most significant product that the NRC produces. As a result, the Agency's data files and the ones provided to us by our stakeholders have a great deal of value. Agency users require mechanisms to store and share large volumes of information with each other and their stakeholders. There is also an ever increasing demand to collaborate on electronic files.

The core storage consists of file servers at each of the regional offices as well as the NRC Storage Area Networks (SAN). (Two other SANs exist in the data center and are part of the optional tasks). Overall, there are approximately five terabytes of storage currently supporting the core tasks, including storage allocated for email.

The offeror shall evaluate the current use of storage at the NRC and make recommendations about appropriate per user network file storage allocations. These recommendations will include definitions of distinct user classes which may have different storage allocation requirements. The offeror shall also recommend an appropriate incremental increase in network file storage allocation per user/per year. The offeror shall provide pricing for this incremental storage. All storage services for the core bid shall be proposed utilizing expandable solutions that will scale up cleanly should optional tasks be exercised for the data center support.

The data management strategy must align with the Continuity of Operations Planning (COOP) and Disaster Recovery (DR) strategy articulated in Section C.5.2.2.5 IT Service Continuity (and Backup and Recovery).

Data Storage Demand Management - A variety of multi-media requirements have emerged that have increased the demand for shared network storage such as the use of digital images for and video recording of inspections, and the need for video training-on-demand. There is an expectation that the need for shared space will grow each and every year. The offeror shall provide a storage solution that can be seamlessly expanded over time.

Data User Class Management - All NRC users do not require the same level of space allocation for Network storage. The offeror shall recommend user storage levels based on roles and responsibilities of the user and an analysis of current storage usage. Access to network storage will be allocated based on user roles. Upon approval of the offeror's

recommendations, the offeror shall provide the requested storage volume for each user class and monitor and report on those allocations to ensure network storage needs are met.

Data File Availability Management - It is critical that the files stored in both personal and shared network storage are both protected and backed-up so that they can be restored when necessary. The offeror shall back-up data files with appropriate frequency to meet the file restoration service level requirements outlined in *Appendix A: SM-SLA-03: File and Print Management*. The offeror shall maintain the back-ups for a minimum of four weeks. In addition, as the Agency's users have become increasingly dispersed, more mobile, and are working more flexible work hours, there is a need to access files from anywhere at any time. The offeror shall provide a storage solution that will allow users to access their files from within the ITI and also from remote locations.

In addition, the offeror shall provide and operate data management tools with the ability to scan for Personally Identifiable Information (PII). PII is information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual. That is, PII is a person's name, in combination with any of the following information: relatives' names, postal address, email address, home or cellular telephone number, personal characteristics, Social Security number, date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or other information that would make the individual's personal identity easily traceable. Note that personal identity is distinct from an individual's professional identity; that is, an employee's name, title, work telephone number, official work location, and work email address are not considered to be PII.

The offeror will provide a recommendation concerning best practice for file retirement and will assist the NRC to develop a policy for retiring files after a recommended period of time.

C.5.1.3.2 Print Management

The offeror shall provide and maintain ability to print electronic documents across the NRC enterprise. The offeror's proposal shall include pricing based on NRC inventory information provided and the offeror's prior experience. Upon award, the offeror shall provide an initial assessment of printer use throughout the Agency and make recommendations for how and what type of printer devices should be used. The offeror shall then make periodic assessments to ensure that an appropriate ratio of printers to users is maintained to meet the Agency's business objectives.

In addition, the offeror shall:

1. Provide all hardware and software supporting the file and print services;
2. Implement automation to allow pro-active, remote monitoring of print devices;
3. Implement secure printing, requiring the physical presence of the user at the printer for the print job to continue;
4. Secure and dispose of all print devices installed with data-bearing drives according to NRC IT security requirements and processes;
5. Maintain print queues;
6. Minimize the amount of time that a user is without access to a given print device (due to either provisioning or repair);
7. Minimize the length and frequency of service outages; and,

8. Minimize the time necessary to provision increased printing capacity when requested by a specific user or when addressing agency-wide requests.

Personal Printer Support – The offeror shall provide best effort support to local printers that are not provided by the offeror. See section C.3.2 Intent for Mutual Cooperation between Offeror and NRC Staff, Item # 5 for more information on best-effort.

Upon completion of their initial assessment, the offeror shall recommend which black & white and color printers are most appropriate for the Agency's business requirements. The offeror shall provide specification recommendations to the NRC Project Officer and a determination will be made by the Agency about which recommendations will be accepted. The offeror will be required to work with the NRC Project Officer and the Office of Administration/Division for Space Planning and Consolidation to make final determinations of printer locations as there are constraints based on power and physical space availability.

Printers must be supported on a three (3) year refresh cycle by the offeror. Offeror-supplied printers will be capable of printing on 8 ½ x 11 and 8 ½ x 14 paper and provide double-sided printing at a minimum. Additionally the offeror shall provide access to printers that are capable of printing 11 x 17 no further than 100 feet from every end-user's on-site workspace.

Printer supplies are provided by another (non-ITISS) contractor. To ensure that this non-ITISS contractor has time to get supplies in stock, the ITISS offeror shall provide the first 90 days of printer ink/toner cartridges when new models are installed and shall not be required for providing any consumables thereafter. Ninety day supplies shall be calculated as sufficient supplies to handle three times the monthly printing capacity of the printer during normal working hours.

C.5.1.3.3 Network Attached Devices Management

Additional, approved, government-owned devices (copiers, digital senders, etc.) currently exist in the environment and are likely to continue during all or part of the ITISS period of performance. The offeror shall provide best-effort support for these devices and shall troubleshoot interface issues between the device and the network. Maintenance of copiers is maintained under a separate contract, and the ITISS offeror is not being required to perform general copier maintenance. However, the offeror shall assist the NRC in identifying and/or correcting problems if a user is unable to use an otherwise-functional, network-attached copier for printing or scanning. Digital senders, or other similar devices will be treated the same as personal printers; the offeror shall install these devices and make best-effort attempt at repairs. See section C.3.2 Intent for Mutual Cooperation between Offeror and NRC Staff, Item # 5 for more information on best-effort.

C.5.1.4 Personal Computing and Related Software Licensing

C.5.1.4.1 Personal Computing

Personal computing devices are the way in which the vast majority of NRC users gain access to the NRC ITI and all of the services that it provides. Due to the high level of automation at the Agency and the fact that information is at the core of our business, these personal computing devices are also the primary tools used to complete the mission of the Agency. For the purposes of this document, "Personal Computer (PC)" refers to the industry standard terminology for laptops and desktops and similar devices and not to equipment owned personally by NRC employees for their own use. In other words, the PCs referred to in this section are provided by either the offeror or the NRC for work purposes.

Different users require different types of PC devices in order to access ITI and other services. Some users are office-bound and a more traditional desktop computing device with a monitor serves their needs. Another group of users spends most of their time traveling, either performing inspections or meeting with global partners. This second group requires a mobile computing solution, but still requires access to many of the services that are available to the office users. Yet another group of users may regularly work in an office, but also works away from the office multiple days a week and requires all of the same services in both locations.

Currently, some remote users access ITI services through the NRC's Remote Access System, which is described in more detail in Section C.5.1.6 *Remote Access*. In addition, The incumbent ISSC contractor currently provisions and maintains an inventory of encrypted MXI Stealth MXP Universal Serial Bus (USB) drives to users to transfer files from one personal computing device to another, including foreign devices. These drives are currently being procured by the NRC through a separate contract. The offeror shall include a proposal to acquire and provide these drives or ones with similar specifications.

These personal computing devices provide a way for each NRC user to access all of the Agency's enterprise services. However, especially when considering mobile computing, these devices also pose several risks to the ITI which must be mitigated in order to protect the Agency's data and infrastructure. Secure computing is of significant importance to the Agency and will drive many decisions about the type of computing devices used and how those devices can be implemented into the infrastructure. Security controls must also include protections to prevent unauthorized computing devices connecting to the NRC ITI. Additionally, as a Federal Government entity, the NRC is required to follow specific security directives and legislation (i.e., Federal Information Security Management Act (FISMA), Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standards, Committee on National Security systems issuances, Federal Desktop Core Configuration (FDCC), etc.). Please see section *C.5.2.2.6 Information Security Management* for additional information on operational IT security requirements.

The NRC also recognizes that personal computing evolves over time, causing at least two significant impacts. The first impact is that the cost of existing computing functionality goes down over time. The second impact is that new personal computing functionality is developed over time which can increase the efficiency and effectiveness of our users in completing the Agency's mission.

It is expected that moving forward, the ratio of desktops and laptops will change as the NRC supports a more mobile workforce. For laptops, an option must be provided with a suitable port replicator, external flat-panel monitor, mouse, and keyboard. The total number of mobile computers versus stationary computers used by the NRC will, in part, be dependent on what is proposed by the offeror.

Prior to award of the ITISS Contract, the NRC is in the process of standardizing to a common laptop program, managed by the incumbent ISSC contractor. The goal of the program is that all personal computing devices in the agency will be managed through the ITISS contract.

Computers must be supported on a three-year refresh cycle and when new must be of sufficiently powerful specifications (CPU, random access memory (RAM), hard drive space, etc.) such that they will be viable during their three-year service life, handling typical corporate applications such as Microsoft Outlook mail, productivity applications (e.g. MS Office) as well as typical web-based applications. Multiple classes of computing devices

shall be supplied by the offeror, which will support each of the user types discussed in the paragraphs above. These devices should be comparable to above-average computers that are available at the time they are placed into service. Personal computing could encompass a wide range of devices including desktops, laptops, thin clients, smart phones, and future technologies that are not currently available on the market. For portable computing devices, the offeror shall offer multiple form factors to meet differing business uses.

Currently, personal computers are provided by the incumbent ISSC contractor through three-year leases. The inventory provided with this SOW provides data on personal computers that are currently in the ITI and when they were last refreshed. The offeror shall include in their proposal provisions for how they will accommodate the transfer of these leases to the ITISS contract or how they intend to absorb the cost of lease termination as a part of their proposed personal computing solution.

Users shall have a reasonable approach to:

1. Record data to portable media (compact discs (CDs), digital video discs (DVDs), etc.)
2. Listen to sound (media files, conferencing, etc.)
3. Attach peripheral equipment (USB ports, etc.)

The offeror shall provide full lifecycle management of personal computing assets from procurement, configuration, delivery, maintenance, refresh, and retirement. The NRC reserves the right to select the ultimate software configurations to be provided.

In addition, the offeror shall:

1. Provide PC devices, including but not limited to desktops, laptops, thin clients, smart phones, peripherals, and other devices requested by users, approved by the NRC Project Officer, and connected to the NRC network;
2. Manage PC device leasing arrangements with third-party hardware vendors; Maintain license agreements with third-party software vendors;
3. Provide on-site maintenance and replacement for all PC devices managed under the contract;
4. Maintain and manage an inventory of all PC devices (both offeror-supplied and Government furnished) managed under the contract; (Note: There are currently Government furnished PC devices, including such things as laptops and monitors, and it is expected that there will be new Government furnished computing devices that will be purchased during the period of performance for this contract which the offeror shall maintain and inventory)
5. Provide a standard environment for NRC employees through the creation, deployment and maintenance of standard workstation images and standard peripheral configurations;
6. Monitor to ensure conformance to the standard environment and report violations;
7. Provide anti-virus, anti-malware, anti-spam, Trojan, and worm detection and prevention software on personal computers and keep virus signature lists up to date. Copies of anti-virus/anti-malware software will be provided to NRC users for working at home use;

8. Provide firewall for PC devices;
9. Maintain patch levels for PC devices and software (all patches must be tested before deployment);
10. Purge data from decommissioned PC devices; devices will be disposed of in an environmentally sound way and based on the security, sensitivity, and associated NRC computer security policies and guidance;
11. Provide PC refresh on a three-year cycle;
12. Provide a pool of encrypted, loaner laptops configured for NRC mobile use per NRC security policies. When the ITISS contract is awarded, it is expected that there will be 100 loaner laptops at headquarters and 80 in the Regions (mostly Region 1), with rebalancing in the Regions over time from current GFE equipment. Laptops with docking stations will also be provided in place of current desktops which will likely impact the total number of loaner laptops to some extent. Alternative solutions suggested by the offeror for managing remote personal computing resource are welcomed;
13. Provide new PC devices over time as needed based on new business requirements and as technology advances to fulfill existing business requirements;
14. Provide global support for hardware maintenance and replacement for NRC users who are traveling abroad with NRC computing devices;
15. Minimize the amount of time that a user is without access to a given hardware unit or software (due to provisioning, repair, replacement, distribution of loaner equipment, or moves – includes account-related incidents/problems). Note that this objective is valid for both offeror-supplied equipment, and for government-furnished equipment (GFE);
16. Minimize time to resolve software uninstalls, and other software-related issues; and,
17. Minimize the length and frequency of service outages.

C.5.1.4.2 Office Productivity Software Deployment

The offeror shall provide full lifecycle management of office productivity software and other personal computer software from procurement, configuration, delivery and retirement based on NRC requirements and direction. Office Productivity software shall be licensed so that NRC users can obtain a copy for installation on a home computer for business use.

C.5.1.4.3 Software License Management

The offeror shall provide software licenses for office productivity software, and manage the procurement and upgrades to that software. The offeror shall also verify that any software requested to be installed on offeror-supplied PC devices is properly licensed. The offeror shall maintain an inventory of all software installed on offeror-provided PC devices and the associated software license information.

The offeror shall report on the use and compliance of all software licenses as requested. The current process (which is expected to continue upon award of this contract) for obtaining and installing user requested software on Agency personal computers is as follows:

1. A user identifies software that they require for meeting a business requirement.
2. The user's manager approves the software purchase.
3. The software is obtained.
4. The user's IT Coordinator makes a formal request to have the software installed.
5. A review is made to determine that the software will not harm the ITI.
6. If approved, the offeror installs the software on the user's workstation.

In addition, the offeror shall procure, supply and manage operating system licenses for all personal computing devices, and keep them patched with current patches. The offeror shall also upgrade to current versions when requested by the NRC. The option to upgrade will be available to the NRC (tested against the NRC environment and ready for migration) within six months of release of the upgrade. Once given approval to upgrade the OS or other offeror-supplied software, the offeror shall manage the entire upgrade, including a clear communications plan, training plan, and customer support. It is expected that the offeror will incorporate the cost of these upgrades into their proposals.

The offeror shall be responsible for ensuring that the software on all offeror-supplied computing devices (desktops, laptops, servers, BlackBerrys etc.) is fully licensed. The offeror shall be financially responsible for any license non-compliance for offeror-supplied software packages. Audits of software licensing will be performed on these devices by an independent verification and validation contractor. The offeror shall bring licenses into compliance for any discrepancies identified in those audits for offeror-supplied software packages.

C.5.1.4.4 Personal Computer Risk Management

The offeror shall manage personal computer risk environment through virus and malware scanning.

In addition, the offeror shall:

1. Provide up-to-date patching for operating systems and productivity software;
2. Provide support of Card Readers for logical (and not physical) access to personal computers in support of HSPD-12;
3. Provide a solution for recovery of lost or stolen hardware (such as Computrace LoJack) to recover equipment that is missing from inventory; and,
4. Provide encryption for data at rest on personal computing devices.

C.5.1.5 Network Components

Disruptions in the network infrastructure are costly, therefore reliable and manageable network components are expected to ensure that enterprise services are available when they are required. Requirements for training through video-on-demand, virtual meetings, and other media-rich collaborations to reduce travel costs and increase productivity also increase the demands on the network infrastructure. All network support functions are to be provided 24 x 7 x 365, including holidays.

Unlike other tasks in the core services section, the network monitoring and asset management tasks require the complete and unified management of all offeror-supplied and

Government-furnished assets attached to the network, including those initially managed under existing contracts outside of the scope of the core ITISS contract. The offeror shall clearly describe how such complete and unified management would be achieved through coordination with other on-site vendors. This shall include the Trusted Internet Connection (TIC). See section *C.5.2.3.3 Service Asset and Configuration Management* of this SOW to obtain a greater understanding of the NRC's requirements related to asset management.

The offeror shall propose a refresh cycle for the components which make up the network backbone. This proposal shall ensure that all of the components are maintained at all times and provide adequate network support. The offeror shall include pricing which is consistent with this network backbone refresh approach.

All changes to the NRC production environment will go through the NRC-approved change management process.

Network Devices – There are several places in this section which refer to network devices. There are many components of the existing NRC ITI which straddle the worlds of networking and system administration. The intent of this wording is to encompass such appliances as firewalls, network filters, load balancers, network accelerators, and devices introduced in the future that are required to manage the NRC ITI. The offeror shall be responsible for maintaining and patching these devices and all of the software running on these devices.

C.5.1.5.1 Network Management

The offeror shall maintain user ability to securely access the network components (including WAN circuits) and services from both within the NRC ITI and remotely.

Encryption is employed on the Multiprotocol Label Switching (MPLS). The offeror shall manage and maintain the related hardware that manages the end-to-end encryption for each connection.

In addition, the offeror shall:

1. Manage, maintain, administer and support the services, network devices, and components that comprise the Agency network infrastructure;
2. Manage, maintain, administer and support the NRC ITI address and Domain Services to provide Internet Protocol (IP) Address management and domain services (nrc.gov, nrc-gateway.gov, and usnrc.gov);
3. Provide protocol management, proxy service, and Public Key Infrastructure (PKI) management;
4. Manage and tracks IP addresses. Support IP version 6 and version 4 addressing and management across the entire NRC ITI (the current network is almost exclusively IPv4, but most of the equipment is IPv6 capable. During the period of performance of the contract, the offeror shall include migration from IPv4 to IPv6);
5. Maintain the capability for all NRC staff to consistently access internal and external multi-media resources;
6. Provide support for Citrix MetaFrame servers. This includes troubleshooting issues for remote users as well as MetaFrame server support;

7. Provide and maintain external access to NRC resources and information for the public and other interested parties with load balancing as needed while maintaining the security of the network infrastructure;
8. Perform account management functions for all infrastructure network devices that require user accounts;
9. Conduct regular performance capacity testing using industry-standard automated tools;
10. Perform impact assessments on all new network technologies introduced in the NRC ITI; and,
11. Interface with long distance and local telecommunications vendors who provide the circuits to troubleshoot incidents and determine root cause of network disruptions.

C.5.1.5.2 Wireless Networking

The offeror shall propose a secure solution in line with Federal and NRC policy for secure wireless networking. If approved, the offeror shall provide wireless networking services and management for secure wireless access points as proposed. The NRC Computer Security Office (CSO) currently has a wireless policy in draft and some of the references used to develop the document are

- National Institute of Standards and Technology (NIST),
- Federal Information Processing Standards (FIPS) (copies of FIPS publications available at the NIST Web site at http://csrc.nist.gov)
  National Institute of Standards and Technology (NIST), Special Publications (SP) (copies available at the NIST Web site at http://csrc.nist.gov), including:

  – SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007
  – SP 800-48 Rev1, Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008 as well as other NRC policies and announcements.

In addition, the NRC Designated Approving Authorities (DAAs) have approved a wireless network solution for the Safeguards LAN (See section C.6.6 Safeguards Local Area Network and Electronic Safe Services). This system includes a thin client approach which prevents data compromise at the client computer and has been deemed an acceptable approach by NRC computer security authorities.

The NRC is planning the re-consolidation of its headquarters into a third building at the main headquarters campus, adjacent to the White Flint Metro station (See section C.6.12 Extraordinary Move Support). This new construction and associated moves (expected in FY 2013) provided an opportunity to introduce new technologies that would reduce long term maintenance and increase ease-of-use for the users.

C.5.1.5.3 Network Asset Management

The offeror shall provide, track, and maintain offeror-supplied and Government Furnished network components and devices which make up the NRC ITI.

C.5.1.5.4 Network Device System Administration

The offeror shall install, support, and maintain network devices, and plan for and respond to service outages and other problems.

In addition the offeror shall:

1. Ensure Pre-Production environment is consistent with the Production environment. (The pre-production environment is a testing and staging environment. It is included in the General Server Environment descriptions in *Section C.4 NRC Environment*. This facility is also referred to in the Integration Task in *Section C.5.1.7.5 Test*);
2. Synchronize client files on remote servers and the failover system;
3. Interface with the helpdesk, network operation center to resolve problems;
4. Coordinate applicable activities with hardware and software maintenance contract personnel; and,
5. Make recommendations for new hardware, software, or procedures that increase performance or availability.

C.5.1.5.5 Maintenance and Patching Management

The offeror shall ensure that network equipment is functioning within manufacturers' operating specifications and current with NRC-approved patches and upgrades according to NRC Change Management procedures. Patching must be maintained to the service levels outlined in *Appendix A: SM-SLA-009: Service Design Lifecycle Support.*

In addition, the offeror shall:

1. Provide software/firmware services including maintenance, deployment, and upgrades for all network infrastructure components and network devices (operating systems, network operating systems, network infrastructure component software, etc.);
2. Provide hardware maintenance services for the Agency-wide NRC ITI;
3. Provide a proposed weekend maintenance schedule;
4. Test all patches before applying them to production;
5. Implement patches defined by the manufacturer/software vendor or the NRC as critical and/or emergency within the timeframes described in the SLRs;
6. Schedule Agency wide infrastructure maintenance services to impact as few users as possible and during the times of least network usage, as much as is feasible not during core hours of operation; and,
7. Update network device and component documentation to reflect current environment. Updates shall include changes to procedures, as-built guides and network diagrams.

C.5.1.5.6 Network Monitoring

The NRC requires vendors to propose a robust, integrated monitoring solution that includes the network, servers, databases, and applications (in terms of application running or not running at least – most home-grown applications are not currently instrumented for more detailed monitoring) and be integrated with the Service Desk management software.

The offeror shall propose a plan for limiting access to the network to only approved devices. Once approved by the NRC, the offeror shall implement this plan.

In addition, the offeror shall:

1. Provide, staff, and manage a Network Operations Center which continuously monitors:
    - The amount of network traffic on all non-secure Agency networks;
    - Types and percentages of protocols traversing the NRC backbone;
    - Types and percentages of services traversing the NRC internet connection;
    - Processor, memory, disk usage percentage, disk write times, required OS and application services; and
    - CPU utilization on all offeror- managed production servers, and other servers as requested by the NRC;
2. Monitor network device logs and review audit trails;
3. Identify and isolate network bottlenecks;
4. Monitor NRC ITI shared network storage for both usage and fragmentation; make recommendations for remediation; and mitigate issues in consultation with the NRC;
5. Leverage technology to increase availability of NRC ITI services;
6. Provide network monitoring, troubleshooting, problem tracking, and resolution for all network components, network devices, and services, 24 x7 x 365;
7. Maintain print queues and solve other problems relative to keeping printers and plotters in working condition;
8. Establish and maintain performance baselines for applications and services, end-user and network response times, and other areas of the infrastructure as requested by the NRC; Once established, the offeror shall alert the NRC whenever there is a variance from these performance baselines;
9. Evaluate trends to determine opportunities for improved performance, provide recommendations for improvements, and implement those changes as requested by the NRC;
10. Monitor for changes to security configurations, service pack applications, etc. that could have security implications and report them to the security group for investigation (See section *C.5.2.2.6 Information Security Management* for additional requirements related to security monitoring and incident response);
11. Provide capacity and performance monitoring and trending reports on all the infrastructure components, and monitor traffic on the Agency non-secured data networks;
12. Ensure that all network events are recorded and filtered, and that the appropriate staff members are notified of the event;
13. Minimize the length and frequency of service outages;
14. Minimize the time necessary to provision increased network bandwidth upon request; and,

15. Minimize the time between a change in ITI status and notification of appropriate NRC personnel.

C.5.1.6 Remote Access

Currently, remote users can access specific application resources from their home computers through a Citrix gateway.

Going forward, the NRC anticipates an environment in which remote computing will be achieved through a combination of the current Citrix gateway and NRC-controlled laptops tunneling into the network securely. The remote computer shall employ a suitable stand-alone/personal firewall installed that supports NRC connection policies. There shall be a mechanism for a minimum critical update level and an associated quarantine area where systems are patched before permitting connectivity. Third-party products are available which can automatically update computers to ensure compliance with a defined security policy even when not connected to the NRC network and should be considered.

The connection between the remote computer and the NRC network must be made through a secure, encrypted Virtual Private Network (VPN) tunnel. The tunnel must be consistent with Federal IT security policy. The VPN shall be configured to require a hardware authenticator (i.e. a hardware "token") which generates a unique key on a timed schedule (approximately every sixty seconds). The remote computer user must enter the generated key along with their password to gain access to the encrypted VPN tunnel.

Split-tunneling, which allows users to access both corporate and local resources simultaneously (such as using the VPN to access the NRC network and in parallel using home-office resources such as local internet access) will be disallowed to maximize security. By tunneling all internet access through the NRC firewall, security standards related to internet access will be enforced.

Access to some applications is also provided through Citrix to both NRC-owned and home-owned computers. The offeror will not be required to physically visit or maintain home-owned computers, but will be required for providing email and telephone support to allow users working from home computers to access Citrix-based applications.

In addition, the offeror shall:

1. Minimize the amount of time that a user is without access to remote connectivity (due to either provisioning or repair); and,
2. Minimize the length and frequency of service outages.

C.5.1.7 Integration

The NRC periodically needs to integrate new software into the ITI and also needs regular updates for patching and updated versions of standard software. Regular patching and updates are part of the natural "seat management" function and shall be provided by the offeror and included in the pricing of the basic seat management function. However as novel technologies emerge and prove to be of benefit to the NRC, the offeror shall work with the NRC to introduce them into the ITI and manage them for the remainder of the contract.

C.5.1.7.1 Project Management

As an Agency largely made up of engineers and scientists, it is vital that up to date IT services are provided to the users to attract and retain the talent we need to accomplish our mission. Designing and implementing new technologies requires thorough project

management discipline. The NRC uses its own Project Management Methodology (PMM – see MD 2.8 http://www.nrc.gov/reading-rm/doc-collections/management-directives/volumes/vol-2.html). The offeror shall use the NRC PMM for projects performed throughout the life of this contract.

In addition the offeror shall:

1. Track project status using NRC Enterprise Project Management (Microsoft Project Enterprise);
2. Follow a proven and documented standard systems Change Management methodology, approved by the NRC for all changes to be made to the NRC ITI;
3. Attend regular NRC meetings to review project schedules, status and resource allocations;
4. Coordinate closely with the other teams (NRC, vendors, contractors, etc.) on projects to ensure smooth transitions;
5. Implement and coordinate the use of NRC Project Management Methodology (PMM) for all IT infrastructure programs and efforts;
6. Minimize time between when a given project update occurs, and the time in which their status in MS Projects is updated; and,
7. Minimize the discrepancy between the milestones defined in MS projects, and the actual delivery of these project milestones.

C.5.1.7.2 Research

Emerging technologies being implemented into existing infrastructure environments requires extensive and thorough research development and testing. The offeror shall perform as the IT systems engineer for the NRC ITI and will provide recommendations, planning, coordination, design and engineering for the IT infrastructure as required for current and future NRC programs, systems, and services.

In addition the offeror shall:

1. Be responsible for providing assessments of the IT infrastructure and making recommendations for new and enhanced systems;
2. Provide short and long range infrastructure strategies for the development, selection, integration, and implementation of infrastructure hardware and software systems,
3. Provide network modeling capabilities to assess the impact of new requirements on network performance;
4. Provide systems architecture, engineering and integration, short and long term planning, research, design, development, performance/capacity planning and modeling/simulation;
5. Analyze, design, and provide recommendations, written reports and white papers on "state of the art" IT technologies applicable to the NRC IT environment as requested by NRC;
6. Perform analyses of commercial off the shelf (COTS) software packages and customized applications for infrastructure use;

7. Provide recommendations to the NRC for testing and integrating new technologies and updates to existing and new systems;
8. Provide guidance and management analysis capabilities to resolve processing and office system operation problems. The areas of expertise will include, but are not limited to: network, server, workstation, portable/mobile, Remote Access System (RAS) and security;
9. Perform research and development, product testing, and evaluations;
10. Conduct performance capacity testing using industry-standard automated tools. Activities shall include, but not be limited to, performing impact assessments on all new technologies introduced in the NRC IT infrastructure. The offeror shall also serve as technical experts in the area of measurement and analysis of LAN, Metropolitan Area Network (MAN), WAN, and Office Automation systems, hardware and software;
11. Perform modeling and simulation using industry-standard automated tools and perform impact assessments on all new technologies introduced in the NRC IT infrastructure; and,
12. Provide IT infrastructure growth and capacity planning recommendations.

C.5.1.7.3 Development

Information technology changes are regularly mandated by federal policy and regulations. The NRC is regularly expected to show progress on a wide variety of IT infrastructure initiatives. New systems and changes must be developed to meet all federally mandated security requirements. The offeror shall provide IT infrastructure development and integration services for the NRC ITI as it evolves over the period of the contract.

In addition the offeror shall:

1. Develop and integrate the IT Infrastructure (network infrastructure, server, workstation, and security) required for current and future NRC projects, systems, and services;
2. Provide technical support for major moves, adds and changes of NRC IT infrastructure and coordination and technical guidance to the NRC's Professional Development Center (PDC) in their preparation of courses related to new and enhanced IT technology as well as other engineering and development requirements as needed;
3. Develop new hardware and software capabilities based upon NRC priorities by integrating and customizing standard off-the-shelf products;
4. Design IT infrastructure systems using the NRC PMM;
5. Develop server hardware standards; design various server/desktop system platforms which adhere to those standards;
6. Develop and maintain an infrastructure forecast, which documents the planned changes to the NRC Infrastructure (desktop/server/network) for the next 36 months;
7. Be aware of and incorporate recommendations for supporting Federal Government IT regulations (Section 508 of the Rehabilitation Act, Paperwork Reduction Act of 1995, etc.) and related requirements;

8. Incorporate engineering and planning techniques to deliver systems that are reliable, flexible, supportable, and expandable;
9. Ensure an effective design, adequate and thorough testing, operational support documentation and the integration of software and hardware that pass production testing for all development activities;
10. Analyze and when appropriate, leverage new network technologies such as: wireless, optical, Gigabit Ethernet, etc;
11. Work with telecommunication vendors/contractors, as necessary, for providing new design, enhancements, and development level support for LAN, MAN, WAN, RAS, and Internet services;
12. Develop and upgrade infrastructure security policies (router passwords, filters, configurations, etc.) as necessary, in coordination with the operational support group;
13. Evaluate and integrate new infrastructure management tools;
14. Develop voice/data/video support and convergence, including media streaming;
15. Develop expert network performance monitoring and analysis;
16. Develop standard file and print server configurations;
17. Develop standard email and application server configurations;
18. Develop Network Operating System (NOS), applications, and utilities as required;
19. Develop standards for supporting network printing and integrated copier services;
20. Provide input to the CSO for the development of server level and user access security policies;
21. Develop standard workstation (desktop/portable/mobile) configurations including hardware, OS, and applications;
22. Develop peripheral hardware standards;
23. Develop monthly desktop update packages (Headquarters [HQ]/Region & Regional Offices and Resident Inspector Sites [RISE]) incorporating updates of desktop software tools;
24. Develop quarterly consolidated desktop images. There are currently four configurations:
    a. Standard - The vast majority of PCs
    b. Standalone - PCs not attached to ITI
    c. Mobile (External) - Laptops which require additional security
    d. RISE - standard + add-on;
25. Develop standards for supporting printing services;
26. Provide software developers with expert knowledge of Microsoft C#.NET expertise and/or java expertise (or similar skills which match the current PC OS) to support the development of workstation upgrades/patches. These software developers shall

have significant experience with Hypertext Markup Language (HTML), Active Server Pages (ASP) and javascript programming. This skill is required to ensure that NRC users have the least amount of disruption when patches and upgrades are being applied to their system; and,

27. Provide expert database developers who can design, develop and administer standard relational database management systems (RDBMS), (i.e. Microsoft SQL Server, Sybase, etc.).

C.5.1.7.4 Implementation

After appropriate and thorough research and development, systems and applications must be implemented into the NRC ITI without causing major disruptions to Agency users. The offeror shall follow ITIL v3 Change, Configuration, Release and Deployment Management best practices and all Federal and NRC policy.

In addition, the Contactor shall:

1. Follow best practice transition techniques that allow for a smooth turnover to the operations teams for operational management;
2. Ensure integration into production without adverse impact on the ITI or NRC ITI users;
3. Ensure performance meets designed standards;
4. Utilize the NRC's Release Management (RM) process or follow a proven and documented methodology, approved by the NRC for all changes to be made to the NRC ITI;
5. For changes so required by the RM process, submit proposed ITI enhancements or modifications to the Operations Change Advisory Board (CAB) for approval prior to implementation;
6. Develop and provide support documentation to the NRC for new and enhanced ITI features for submission to the CAB, which has overall responsibility for evaluating and approving change requests;
7. Review, as necessary, Environmental Configuration Control Board (ECCB) submissions to assess impacts on the infrastructure;
8. Update all configuration information within 24 hours of implementing into the NRC ITI;
9. Minimize the discrepancy between Request for Change (RFC) records and actual change requests;
10. Minimize the number of failed RFCs (including both normal and emergency changes); and,
11. Minimize the number of changes that are not associated with an approved RFC.

C.5.1.7.5 Test

The NRC regularly adds and changes technologies in the NRC ITI. However, as existing IT services are vital to the day-to-day productivity of NRC users, it is essential that the introduction of these changes does not disrupt normal Agency operations.

Therefore, all modifications to the NRC ITI must be thoroughly tested in the Agency's test environment and appropriate precautions must be taken to mitigate any disruptions that they might introduce. The offeror shall provide a "best value" test environment that replicates the production environment so that tests can be as accurate as possible and real problems can be identified and corrected. Although individual IT system owners must take the responsibility to move their systems through this process, the offeror shall help them to succeed in this endeavor by providing expertise in testing and resolving common issues.

The test facility currently operates on a separate network not accessible to the production environment. It is not currently accessible from all locations.

Testing Management – The offeror shall provide the technical environment for and maintain the ability to test all new applications and hardware to ensure a smooth transition into the NRC ITI.

In addition, the offeror shall:

1. Maintain the test environment network including infrastructure, servers and applications with up-to-date patching at the same level as the NRC ITI;
2. Ensure that the test environment is segregated from the production environment;
3. Operate and manage the test environment to support testing, network performance impact analysis, network modeling and simulation, load testing, application testing, Rehabilitation Act Section 508 testing, integration, demonstration, product briefings, evaluation and orientation/training for all COTS and custom services and applications to be integrated into the infrastructure;
4. Ensure application and hardware integration into production without adverse impact on the infrastructure;
5. Provide non-production data sets for testing systems. No production data shall be used in the test environment;
6. Provide recommendations for a solution that allows users to test applications from anywhere within the ITI by accessing a virtual desktop within the test environment without any risk to the ITI production environment. The NRC reserves the right to decline the recommended solution; therefore, the vendor will provide this capability upon request and approval by the NRC. The recommendation will also need to be approved by the NRC prior to production implementation;
7. Manage a schedule of test environment availability, publish that schedule, and work with customers in scheduling the use of the environment;
8. Minimize the number of incidents associated with any change to the live environment;
9. Maximize the availability of the test environment; and,
10. Minimize the incidents/problems/errors that are discovered found in the live environment, after release

C.5.1.8 High Performance Computing

The NRC performs both independent and collaborative modeling to examine different approaches to the management of radioactive materials. The ultimate objective of the studies is to ensure that materials are securely managed and pose low or no risk to the

population at large. High performance computing has made it possible to create simulations which mimic real-life situations without the risk of endangering anyone.

Because Federal agencies and universities are often involved in this same pursuit, the NRC must be able to collaborate with these partners and their foreign networks. This creates risks for the primary ITI which must be mitigated through appropriate security controls. Currently, this is being accomplished with the high performance computing zone, a virtual LAN). The offeror shall manage the high performance computing zone and data center.

In addition, the offeror shall:

1. Provide system administration and operational support of the high performance computing zones and data center. Due to their nature, some programs may require a longer execution time, and all system maintenance activities such as virus scanning, server backups, patches, troubleshooting, rebooting, data file backup and restoration, etc. shall follow procedures separately established specifically for each of the systems in the high performance computing zones and data center upon request by designated NRC staff;
2. Provide assistance in the planning, development, design, and implementation of the effort to consolidate high performance computing at the agency;
3. Provide end user support by responding to requests concerning the system software, hardware, network, and information security of the high performance computing zones and data center;
4. When requested by end users, provide application software support of installation, setup, configuration and other services to coordinate with third-party vendors and providers;
5. Provide telecommunication and network support that may include, but is not limited to, performance throughput, large data file transfers, information security to protect certain proprietary data files, interfaces/access to the NRC Production Operating Environment (POE) and the Internet, etc.;
6. Provide assistance and support in the development and maintenance of all system security related documentation of the high performance computing zones and data center. This may includes, but is not limited to, responding to audit, information security compliance, and other data call requests in accordance with Agency requirements; and,
7. Minimize the length and frequency of service outages.

C.5.2 Service Delivery and Management Responsibilities

This section describes responsibilities of the NRC and the offeror within the framework of ITIL V3 best practices. All responsibilities described herein apply to the basic infrastructure support services described in C.5.1 Basic Infrastructure Support Services and any optional services described in C.6 Optional Services that are exercised. The offeror shall describe their ITIL v3 experience in the context of each of these sections and shall also describe how they will assist the NRC in maturing our service delivery. The offeror shall also describe their efforts in achieving ISO 20000 certifications, as appropriate.

All service delivery for core and optional tasks shall be in accordance with the NRC Enterprise Architecture and Security Architecture guidelines. The offeror shall seek out these guidelines prior to proposal of new technologies.

C.5.2.1 Service Strategy

Service Strategy describes how the service provider will efficiently fulfill the needs of the stakeholders, both purchasers and users of the services. It is the provider's approach to delivering value and fulfilling their strategic purpose in the organization. All service strategy discussions shall be in the context of business needs. Most Service Strategy work will be performed by the NRC.

C.5.2.1.1 Strategy Generation

C.5.2.1.1.1 NRC Responsibilities

The NRC will retain all responsibility for strategy generation tasks other than those listed in the next section.

C.5.2.1.1.2 Offeror Responsibilities

Initially, the NRC will meet with the offeror quarterly to discuss changes to the service strategy. The offeror will provide a quarterly report to the NRC detailing recommendations for changes and updates to the Service Strategy based on observations and requests for recommendations from the NRC. Requests shall be furnished to the offeror by the NRC no later than the second week of the quarter. This can also be used as the forum in which the offeror can request changes in behavior and/or the environment that would provide them cost savings. When appropriate, probably during the second year of the base period of the contract, these strategy recommendations will be reduced to twice annually, and may be further reduced based on direction from the NRC Project Manager.

C.5.2.1.2 Financial Management

C.5.2.1.2.1 NRC Responsibilities

The NRC is ultimately responsible for Financial Management.

C.5.2.1.2.2 Offeror Responsibilities

The offeror shall provide cost-effective financial IT stewardship safeguarding against waste, fraud and abuse of IT resources and assets.

In addition, the offeror shall:

1. Provide detailed cost reports to use in the budgeting and reconciliation processes; and,
2. Report monthly progress and financial performance for all activities under the contract in the Monthly Technical and Financial Status Report.

C.5.2.1.3 Service Portfolio Management

C.5.2.1.3.1 NRC Responsibilities

The NRC is responsible for Service Portfolio Management except as noted in the next section.

C.5.2.1.3.2 Offeror Responsibilities

The offeror will recommend more cost-effective approaches to service provisioning and the service portfolio as they are identified.

C.5.2.1.4 Demand Management

C.5.2.1.4.1 NRC Responsibilities

The NRC is primarily responsible for Demand Management, supported by the offeror.

C.5.2.1.4.2 Offeror Responsibilities

The offeror will report on usage and specifically highlight areas where savings can be realized or capacity extended by influencing the users' demand for resources.

C.5.2.2 Service Design

C.5.2.2.1 Service Catalog Management

C.5.2.2.1.1 NRC Responsibilities

The NRC is responsible for determining what will be in the service Catalog, as a subset of the Service Portfolio identified as part of the Service Strategy lifecycle activities. The NRC is also responsible for defining the business rules associated with workflow for automated management of catalog requests.

C.5.2.2.1.2 Offeror Responsibilities

NRC users need a comprehensive list of all IT services that are available to them. This list will include information about the service including a comprehensive description, the agreed upon service levels, how to obtain the service, who is authorized to obtain the service, service contacts and associated costs and/or chargeback.

The offeror shall provide and implement software to manage the service Catalog which will provide direct links into their service request fulfillment system to provide seamless capabilities to NRC requestors. The offeror shall be responsible for providing role based authorization for the adjustment of NRC defined business workflows into the Service Catalog.

The offeror shall provide software to allow users a self service mechanism to request services found in the service Catalog, and to track the status of their requests. The software will provide workflow for the management of the requests.

The offeror shall update and maintain the information in the service Catalog at the direction of the NRC.

The offeror shall be specific about the software that will be used to provide the service Catalog and their experience utilizing that software with other customers.

The offeror is responsible for maintaining, updating, and ensuring the on-line availability of the catalog.

Access to the service Catalog shall be made available through the NRC intranet and shall be formatted consistently with NRC Web standards and formats.

When there is a change to any process or procedure supporting an ITI service, the procedural documentation within the Service Catalog will be updated within 3 business days of the change.

In addition, the offeror shall:

1. Maximize the availability of the service catalog; and,
2. Minimize the discrepancy between the information contained in the service catalog and actual services provided.

C.5.2.2.2 Service Level Management

C.5.2.2.2.1 NRC Responsibilities

The NRC is ultimately responsible for Service Level Management. Appendix A provides all SLRs related to the ITISS contract.

C.5.2.2.2.2 Offeror Responsibilities

The offeror shall support the NRC to adjust performance measures as appropriate to ensure customer satisfaction and to ensure that NRC user requirements are being met. There will be semi-annual meetings at which Service Levels will be reviewed, discussed, negotiated, and potentially modified.

The offeror shall also be responsible for providing all detailed data, reports, and other information used to develop the service levels reported for each reporting period and for providing their analysis of their performance against the Service Level Requirements.

C.5.2.2.3 Capacity Management

C.5.2.2.3.1 NRC Responsibilities

The NRC is responsible for setting performance and availability targets and for reviewing the capacity plan and capacity models with the offeror. The NRC is responsible for concurring with these planned items and the decisions to furnish further capacity. The NRC is also responsible for providing the offeror with estimates on the size of the NRC staff and notification of unusual circumstances that may impact capacity. The NRC is also responsible for enforcing the non-technical components of rules around disk space limitations, etc. (ensuring staff abide by policy). However, the offeror is primarily responsible for capacity management to ensure the targets are met and that proactive planning and modeling are done.

C.5.2.2.3.2 Offeror Responsibilities

Quarterly, the offeror will update a capacity plan and capacity models to forecast current and future (to one year out) technical capacity needs (space, computing power, bandwidth, etc) to include human resource capacity on the service desk and Tier 1 support. The offeror will ensure that performance and availability targets are met, and lead the diagnosis and resolution of incidents and problems related to capacity.

The offeror will recommend the most cost-effective capacity plan for the NRC. As such, the offeror shall be cautious about not providing more capacity than is appropriate for underlying NRC business requirements.

C.5.2.2.4 Availability Management

C.5.2.2.4.1 NRC Responsibilities

See Capacity Management.

C.5.2.2.4.2 Offeror Responsibilities

The offeror shall sustain availability of NRC ITI to ensure users can access network services and applications and complete their work.

In addition, the offeror shall:

1. Identify and recommend measures to optimize network or server performance, and provide network expansion, reconfiguration or redesign based on historical network trends and future business requirements;
2. Review network infrastructure configurations and perform routine configuration audits on a continual basis to ensure consistency and standards of the NRC ITI are maintained;
3. Work cooperatively with NRC staff and other NRC Contractor support staff to resolve network problems;
4. Provide input for communications to ITI users about system impacts and outages and to keep them informed about updates;
5. Provide web accessible network health and performance information to specific NRC staff desktops on a real time basis for all network infrastructure components, services and systems;
6. Schedule and provide routine preventive maintenance to assure the highest quality output, and to prolong the useful life of equipment as required by the manufacturer;
7. Provide reports showing any ITI component downtime. This report includes duration, cause, resolution impediment factors, and the names and the offices of the affected users;
8. Provide any external trouble ticket information that is obtained when an outside vendor (e.g. Verizon) is contacted due to a circuit issue. This shall include the date/time the ticket was opened, the ticket number, and the expected resolution time. For any service impacting outages, a Situation Report will be required to provide 30-minute status updates to select individuals such as the Office of Information Services (OIS) Director and Infrastructure & Computer Operations Division (ICOD) Director; and,
9. Maintain activity, problem, equipment failure, or other logs to record irregularities in normal facility operations.
10. Provide lessons learned input and documentation to the NRC to ensure that preventable incidents and outages are avoided.

Network Traffic Management - The offeror shall monitor and evaluate the amount and type of traffic on the NRC ITI and develop solutions to reduce traffic-caused delays. See section *C.5.1.5.1 Network Management* of this SOW for more details of NRC's requirements for Network Management.

Network Tomography[1] - The offeror shall Monitor the health of NRC ITI links in real-time for congestion and delays.

C.5.2.2.5 IT Service Continuity (and Backup and Recovery)

The NRC is engaged in ongoing activities in enhancing and expanding disaster recovery capabilities for the Agency's portfolio of "business critical" IT assets and data systems. Development of the NRC Disaster Recovery Plan (DR Plan) was completed in July 2009 which outlines the Agency's requirements and provides a roadmap supporting a phased approach to full disaster recovery implementation. As implementation of the plan progresses, the offeror shall assist in the planning, deployment, and maintenance and support of the various IT systems outlined in the DR Plan.

C.5.2.2.5.1 NRC Responsibilities

The Agency maintains continuity plans to continue critical operations in the event that the primary systems in support of those critical operations are unavailable. The Agency has also been evaluating another tier of business processes (or Vital Business Functions) that include significant mission functions and supporting functions that need to be in place in order to carry out the Agency's mission. The Agency must be able to recover these mission support areas within a reasonable timeframe.

IT Service Continuity (ITSCM) supports NRC Business Continuity Planning by ensuring that the required IT technical services, infrastructure, and telecommunication services can be resumed within the agreed upon timeframes. Technical services include the related technology components such as networks, computer systems, data repositories, and telecommunications as well as technical staff and the service desk. Periodic testing of the ITSCM shall be conducted to ensure the completeness of the ITSCM Plans. The NRC is responsible for driving that testing and for providing appropriate business support to the testing effort.

The Agency will ensure that the guidance, assets, and resources are documented and available to support all Agency-wide disaster recovery requirements. The Agency will be responsible for establishing and maintaining contractual relationships with alternate site service providers; establishment and maintenance of Service Level Agreements (SLAs) with other Government Agency's hosting applications and systems used by NRC; and monitoring SLA status of offeror performance of disaster recovery tasks.

C.5.2.2.5.2 Offeror Responsibilities

The offeror shall assist the NRC in the management of the overall plan including risk assessments, development of appropriate countermeasures, and recovery strategies.

---

[1] Network tomography is the study of a network's internal characteristics using information derived from end point data. The word tomography is used to link the field, in concept, to other processes that infer the internal characteristics of an object from external observation, as is done in magnetic resonance imaging or positron emission tomography (even though the term tomography strictly refers to imaging by slicing). The field is a recent development in electrical engineering and computer science, founded in 1996. Network tomography advocates believe that it is possible to map the path data takes through the Internet by examining information from "edge nodes," the computers where data is originated and requested from. - Yardi, Y. (1996). "Network Tomography: estimating source-destination traffic intensities from link data". J. Am. Statistics Association 91: 365–377.

IT Service Continuity Operational Management – The offeror shall execute operational activities for ITSCM including user and technician training and education, preparation of plans, periodic testing of the ITSCM recovery plans, and periodic audit and review of the plan, testing, and documented results.

In addition, the offeror shall:

1. Provide metrics on the status of testing of each service continuity plan to ensure the viability of the plans;
2. Provide metrics on the accuracy of the offeror's contact information list, including the sampling date, number sampled and the number of correct contacts;
3. Provide a testing and auditing schedule for all Services indentified in the ITSCM plan;
4. Incorporate an indicator of the Vital Services covered by the ITSCM into the service Catalog;
5. Design and implement system backup, restore and recovery plans and procedures that include encryption of backup data;
6. Enhance and/or modify backup and recovery programs as needed;
7. Perform daily backups of all file servers and application servers (for all systems);
8. Provide routine removal and retention of backup media to off-site storage at a remote location other than NRC headquarters or the Regional Office;
9. Prevent loss of information during all operations and maintenance activities by taking steps to protect and, at the NRC's direction, restore, as necessary, any information residing in the equipment being maintained;
10. Provide restoration services with no significant impact to NRC ITI or end-user performance from backup copies;
11. Manage, support, maintain and execute the NRC's Network Continuity of Operations (COOP) plans and COOP sites;
12. Maintain and perform specified disaster recovery and failover procedures;
13. Provide support for failing over the production environment to the warm standby environment located in another NRC facility;
14. Perform daily replication to the warm standby environment, and ensures data synchronization to backup site was successful;
15. Update internal DNS to enable internal routing, and the fail-over process to backup units when changes occur;
16. Update failover documentation as necessary to reflect current operational configurations;
17. Encrypt back-up data based on federal government encryption compliance requirements (e.g., FIPS 140-1); and,
18. Minimize the time between the planning and testing of IT Service Continuity Plans.

Specific to the systems identified in the DR Plan, the offeror shall provide ongoing maintenance and support of applications, systems, communications and infrastructure components, security, training, and documentation for systems identified in the DR Plan. The support is intended to assist NRC with implementing and maintaining systems included in the DR environment. Tasks shall include but not be limited to:

1. Assisting with detailed preparation, configuration, testing, and deployment of systems/applications identified in the NRC DR Plan not "DR-enabled" prior to contract award;
2. Ongoing operation and support of systems/applications that have been DR-enabled prior to contract award;
3. Designing and implementing of system backup, restore and recovery plans and procedures;
4. Maintaining and modifying backup and recovery documentation and procedures as technical and procedural changes occur;
5. Performing daily backups of all file servers and application servers specified in the DR Plan;
6. Providing routine removal and retention of backup media (providing media to the offsite storage vendor) a remote location other than NRC headquarters or the Regional Office;
7. Participating in scheduled disaster recovery testing to ensure proper failover and recovery of systems/applications;
8. Performing daily replication to the warm standby environment, and ensuring data synchronization to backup site was successful as specified in the DR Plan;
9. Providing updates to the internal DNS to enable internal routing, and the fail-over process to backup units when changes occur; and,
10. Assisting in site visits to alternate site locations to ensure that both the production and alternate sites are properly configured and aligned at all times.

C.5.2.2.6 Information Security Management

C.5.2.2.6.1 NRC Responsibilities

At the core of the Agency's mission is to ensure the safe and secure handling of radioactive materials. Since its creation, the NRC has always sought to appropriately protect its information resources. The increase in computerization has caused the majority of that information to exist in electronic form as data records and files. The sophistication and frequency of malicious activity targeting the Agency has also increased.

These forces combined with the need for Agency users to stay connected with our stakeholders and partners through the Internet pose a significant risk to the Agency if left unmitigated. A thorough, aggressive strategy must be instituted to protect the Agency's information resources. It is expected that this strategy will need to be adjusted and enhanced over time as the sophistication of malicious activity increases.

The NRC is ultimately responsible for Information Security Management, but the offeror will play a vital role in helping to achieve the NRC's goals.

C.5.2.2.6.2 Offeror Responsibilities

IT Security Program Management

The offeror shall advise on, deliver and manage a wide-ranging IT security program to prevent, detect, and respond to IT security incidents.

In addition, the offeror shall:

1. Maintain adequate physical and logical security measures for network infrastructure components, devices, systems and services in conjunction with the Office of Administration (ADM) and the Computer Security Office (CSO). The Office of Administration maintains building security at headquarters and coordinates physical security throughout the Agency. They maintain the policy. However, certain physical security requirements (as mandated by FISMA and NRC IT security policy) exceed building security.

   The offeror must provide these additional security controls, but work with NRC Office of Administration. For example, certain areas maintained by the offeror (i.e. Data Center, SLES server room) require logging of personnel as they enter and exit the space, for which the offeror shall be responsible. Another possible example is that the offeror may propose an external facility to NRC headquarters to manage some segment of the ITISS contract. In this case, the offeror shall be responsible for meeting all Federal and NRC physical security control requirements;

2. Provide industry best practice security architecture recommendations to the NRC;
3. Implement, maintain, and administer appropriate security measures for all data network infrastructure components, devices, systems and services;
4. Perform account management functions for all infrastructure systems that require user accounts; Maintain a tiered account access model;
5. Perform patch management, including:
   a. subscription to the vendor hardware/software notification sites for the latest patch notifications
   b. consideration of the severity of the vulnerability during determination of the timeliness of applying the patch
   c. a schedule for applying patches
   d. testing of patches before applying to production
   e. verification that patches were applied

   Patching must be maintained to the service levels outlined in *Appendix A: SM-SLA-009: Service Design Lifecycle Support.*
6. Maintain, verify and monitor baseline configuration for all components;
7. Perform vulnerability management containing regularly scheduled internal vulnerability audits and a process in place to regularly correct discovered vulnerabilities and configuration discrepancies;
8. Participate in the development of system packages used to obtain an authority to operate and assist in independent evaluation of security requirements;

9. Understand, support, and implement the IT security requirements for certification and accreditation (C&A) of Federal Government systems;
10. Ensure offeror employees complete initial and annual security awareness training;
11. Provide privileged users with additional security training specific to their duties;
12. Manage mitigating controls such as anti-virus, anti-malware, and anti-spam to reduce user exposure to malicious attacks. Provide anti-virus software on Agency personal computing devices and network infrastructure devices, servers, and systems to prevent data file damage and corruption; Maintain currency of virus definitions; Provide automated distribution of updated virus definitions to Agency desktop computers and infrastructure devices; Perform daily virus scans on high performance computing servers. All virus scan activities shall follow the procedures separately established specifically for each of the systems in the high performance zones and data center;
13. Gather and analyze statistical security information and provides recommendations to improve and enhance network security;
14. Perform periodic security assessment to ensure compliance with security procedures and processes and make report available to NRC IT security oversight bodies;
15. Minimize the time between the vendor release of, and installation of, service/security/antivirus/spyware patches/updates; and,
16. Minimize the time to update computers that are not in antivirus/spyware compliance.

Performance criteria for security operations, security management, and vulnerability testing by the offeror shall be aligned with the National Institute of Standards and Technology (NIST) Special Publications (SP) found at http://csrc.nist.gov/publications/PubsSPs.html and NRC Management Directives, Computer Security Officer Security Policies, Procedures, Standards, and Guidance.

See sections *C.5.2.5.1 Centralized Reporting* and *Appendix E: Reporting Requirements* for a greater understanding of NRC's general reporting requirements.

Network Security Center Management

The offeror shall staff and operate a facility to proactively monitor, avoid, report, mitigate, and respond to IT security incidents.

In addition, the offeror shall:

1. Manage, maintain, administer and support the NRC Internet firewall as a system including a set of router filters that provide the first line of defense from the Internet;
2. Manage, maintain and administer other security systems, including log management, proxy, vulnerability scanning, traffic analysis devices to provide reporting, analysis and alerting of emerging security issues, as well as the ability to implement mitigating controls;
3. Provide, manage, maintain, and operate an automated tool to audit NRC ITI system logs; evaluate and report on security events monitored in those logs as determined by NRC policy and IT security oversight bodies;

4. Manage, maintain, and operate an automated tool to monitor changes to system baseline configuration settings and report on events as determined by NRC policy and IT security oversight bodies;
5. Provide notification of IT security incidents to the NRC and assist the NRC in all activities related to those incidents;
6. Operate and manage the demilitarized zone (DMZ), an essential part of the NRC firewall design, to provide the isolation of foreign networks that are interconnected with the NRC from the internal NRC network;
7. Develop and upgrade infrastructure security procedures (router passwords, filters, configurations, etc.) as necessary, in coordination with the operational support group in accordance with security policies;
8. When security incidents occur, provide information on the likely risk, severity, and impact (i.e. which systems or applications effected, which users effected, etc.) of each security incident; and,
9. Maximize the value of the information provided by the offeror to the NRC by correlating related incidents

IT Security Monitoring

Review and evaluate logs, events, and specialized tools to identify significant security incidents and develop and implement appropriate responses to those security incidents.

In addition, the offeror shall:

1. Develop and maintain auditing systems and take the necessary actions to prevent and stop unauthorized access and/or suspicious activity;
2. Perform verification of perimeter router policies; configure firewall or network sensor to alert for unauthorized access attempts and privilege escalation; and perform routine review of Host Intrusion Detection system (HIDs), Network Intrusion Detection systems (NIDs), and firewall rules for accuracy, efficiency and their ability to withstand new attacks;
3. Maintain systems that automatically examine network access logs for signs of unauthorized access, intrusion or suspicious activities;
4. Log all access attempts by NRC users, offeror users, and administrators;
5. Share all relevant threats, vulnerabilities, or incidents immediately with designated NRC personnel;
6. Provide the Government access to security-related audit trails/logs;
7. Spot trends, identify problem areas, and ensure that policies and administrative actions are handled in a consistent manner;
8. Provide reports such as system audit logs, password control lists, user access logs and reports, reports on periodic security audits, and reports on unauthorized access attempts;
9. Routinely check that no new ports, protocols, or services are activated without approval by a configuration management board (See section *C.5.2.3.3 Service Asset*

and Configuration Management of this SOW to obtain a greater understanding of the NRC's requirements related to asset management.);

10. Develop and maintain strong two-factor authentication for management and administrator access of NRC systems. Least privilege for these accounts are to be provided such that these individuals have a user and a management / administrative account with the higher privileged account used only for management and or administrative functions with all privileged access logged and reviewed by the NRC security officials and make these reports available when requested by the NRC;
11. Identify and prevent any non-ITI devices (including computers, USB drive, peripherals, etc.) attempting to attach to the ITI;
12. Minimize the time to escalate and investigate security incidents once identified; and
13. Ensure the offeror's compliance with the NRC formal change and configuration management processes; the offeror shall not make changes without using this process.

Security Compliance Planning and Management

The offeror agrees to insert terms that conform substantially to the language of the IT security requirements, excluding any reference to the Changes clause of this contract, all subcontracts under this contact.

For unclassified information used for the effort, the offeror shall provide an information security categorization document indicating the sensitivity of the information processed as part of this contract if the information security categorization was not provided in the statement of work. The determination shall be made using NIST SP 800-60 and must be approved by CSO. The NRC contracting officer and project officer shall be notified immediately if the offeror begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the NRC contracting officer and project officer shall be notified immediately if the offeror begins to process information at a more restrictive classification level.

All work under this contract shall comply with the latest version of all applicable guidance and standards. Individual task orders will reference applicable versions of standards or exceptions as necessary. These standards include, but are not limited to, NRC Management Directive 12.5 Automated Information Security Program, and National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS), and Committee on National Security Systems (CNSS) policy, policy, directives, instructions, and guidance. This information is available at the following links:

NRC Policies, Procedures and Standards (CSO internal website):

http://www.internal.nrc.gov/CSO/policies.html

All NRC Management Directives (public website):

http://www.nrc.gov/reading-rm/doc-collections/management-directives/

NIST SP and FIPS documentation is located at:

http://csrc.nist.gov/

CNSS documents are located at:

http://www.cnss.gov/

When e-mail is used, the offeror shall only use NRC provided e-mail accounts to send and receive sensitive information (information that is not releasable to the public) or mechanisms to protect the information during transmission to NRC that have been approved by CSO.

All offeror employees must sign the NRC Agency Rules of Behavior for Secure Computer Use prior to being granted access to NRC computing resources.

The offeror shall adhere to NRC policies, including but not limited to:

- Management Directive 12.5, Automated Information Security Program
- Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
- Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
- Computer Security Information Protection Policy
- Remote Access Policy
- Use of Commercial Wireless Devices, Services and Technologies Policy
- Laptop Security Policy
- Computer Security Incident Response Policy

The offeror will adhere to NRC's prohibition of use of personal devices to process and store NRC sensitive information.

All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the sensitivity level of the information being processed.

The offeror shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the offeror's computer facility, and the offeror will retain no NRC data within 30 calendar days after contract is completion. Until all data is purged, the offeror shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

When offeror's employees no longer require access to an NRC system, the offeror shall notify the project officer within 24 hours.

Upon contract completion, the offeror shall provide a status list of all NRC system users and shall note if any users still require access to the system to perform work if a follow-on contract or task order has been approved by NRC.

The offeror shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any security controls or countermeasures either designed or developed by the offeror under this contract or otherwise provided by the NRC.

Any IT system used to process NRC sensitive information shall:

- Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to provide.

- Be able to authenticate data that includes information for verifying the claimed identity of individual users (e.g., passwords)
- Protect authentication data so that it cannot be accessed by any unauthorized user
- Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user
- Report to appropriate security personnel when attempts are made to guess the authentication data weather inadvertently or deliberately

Any offeror system being used to process NRC data shall be able to define and enforce access privileges for individual users. The discretionary access controls mechanisms shall be configurable to protect objects (e.g., files, folders) from unauthorized access.

Any offeror system being used to process NRC data shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

The offeror shall only use NRC approved methods to send and receive information considered sensitive or classified. Specifically,

- **Classified Information** - All NRC Classified data being transmitted over a network shall use NSA approved encryption and adhere to guidance in MD 12.2 NRC Classified Information Security Program, MD 12.5 NRC Automated Information Security Program and Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing.
- **SGI Information** – All SGI being transmitted over a network shall adhere to guidance in MD 12.7 NRC Safeguards Information Security Program and MD 12.5 NRC Automated Information Security Program. SGI processing shall be only within facilities, computers, and spaces that have been specifically approved for SGI processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The offeror shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.

Separation of duties for offeror systems used to process NRC information must be enforced by the system through assigned access authorizations.

The mechanisms within the offeror system or application that enforces access control and other security features shall be continuously protected against tampering and/or unauthorized changes.

The offeror shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).

The offeror shall ensure that the software does not contain undocumented functions and undocumented methods for gaining access to the software or to the computer system on which it is installed. This includes, but is not limited to, master access keys, back doors, or trapdoors.

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: http://www.internal.nrc.gov/CSO/standards.html .

All media used by the offeror to store or process NRC information shall be controlled in accordance to the sensitivity level.

The offeror shall not perform sanitization or destruction of media approved for processing NRC information designated as SGI or Classified. The offeror must provide the media to NRC for destruction.

The offeror must adhere to NRC patch management processes for all systems used to process NRC information. Patch Management reports will made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

For any offeror system used to process NRC information, the offeror must ensure that information loaded into the system is scanned for viruses prior to posting; servers are scanned for viruses, adware, and spyware on a regular basis; and virus signatures are updated at the following frequency:

- 1 calendar day for a high sensitivity system
- 3 calendar days for a moderate sensitivity system
- 7 calendar days for a low sensitivity system

All system modifications to classified systems must comply with NRC security policies and procedures for classified systems, as well as federal laws, guidance, and standards to ensure Federal Information Security Management Act (FISMA) compliance.

The offeror shall correct errors in offeror developed software and applicable documentation that are not commercial off-the-shelf which are discovered by the NRC or the offeror. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause in Section I, FAR 52.233-1, incorporated by reference in the contract.

The offeror shall adhere to the guidance outlined in NIST SP 800-53, FIPS 200 and NRC guidance for the identification and documentation of minimum security controls.

The offeror shall provide the system requirements traceability matrix at the end of the initiation phase, development/acquisition phase, implementation/assessment phase,

operation & maintenance phase and disposal phase that provides the security requirements in a separate section so that they can be traced through the development life cycle. The offeror shall also provide the software and hardware designs and test plan documentation, and source code upon request to the NRC for review.

All development and testing of the systems shall be protected at their assigned system sensitivity level and shall be performed on a network separate and isolated from the NRC operational network.

All system computers must be properly configured and hardened according to NRC policies, guidance, and standards and comply with all NRC security policies and procedures as commensurate with the system security categorization.

All offeror provided deliverables identified in the project plan will be subject to the review and approval of NRC Management. The offeror will make the necessary modifications to project deliverables to resolve any identified issues. Project deliverables include but are not limited to: requirements, architectures, design documents, test plans, and test reports.

Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 and must be operated in FIPS mode. The offeror shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

The offeror must ensure that the system will be divided into configuration items (CIs). CIs are parts of a system that can be individually managed and versioned. The system shall be managed at the CI level.

The offeror must have a configuration management plan that includes all hardware and software that is part of the system and contains at minimum the following sections:

- Introduction
  - Purpose & Scope
  - Definitions
  - References
- Configuration Management
  - Organization
  - Responsibilities
  - Tools and Infrastructure
- Configuration Management Activities
  - Specification Identification
  - Change control form identification
  - Project baselines
- Configuration and Change Control
  - Change Request Processing and Approval
  - Change Control Board
- Milestones
  - Define baselines, reviews, audits
- Training and Resources

The Information System Security Officer's (ISSO's) role in the change management process must be described. The ISSO is responsible for the security posture of the system. Any

changes to the system security posture must be approved by the ISSO. The offeror should not have the ability to make changes to the system's security posture without the appropriate involvement and approval of the ISSO.

The offeror shall track and record information specific to proposed and approved changes that minimally include:

Identified configuration change
Testing of the configuration change
Scheduled implementation the configuration change
Track system impact of the configuration change
Track the implementation of the configuration change
Recording & reporting of configuration change to the appropriate party
Back out/Fall back plan
Weekly Change Reports and meeting minutes
Emergency change procedures
List of team members from key functional areas

The offeror shall provide a list of software and hardware changes in advance of placing them into operation within the following timeframes:

- 30 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 10 calendar days for a low sensitivity system

The offeror must maintain all system documentation that is current to within:

- 10 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Modified code, tests performed and test results, issue resolution documentation, and updated system documentation shall be deliverables on the contract.

Any proposed changes to the system must have written approval from the NRC project officer.

The offeror shall maintain a list of hardware, firmware and software changes that is current to within:

- 15 calendar days for a classified, SGI or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The offeror shall analyze proposed hardware and software configurations and modification as well as addressed security vulnerabilities in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system

- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The offeror shall provide the above analysis with the proposed hardware and software for NRC testing in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The offeror shall demonstrate that all hardware and software meet security requirements prior to being placed into the NRC production environment.

The offeror shall ensure that the development environment is separated from the operational environment using NRC CSO approved controls.

The offeror shall only use licensed software and in-house developed authorized software (including NRC and offeror developed) on the system and for processing NRC information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the NRC Chief Information Security Officer (CISO).

The offeror shall provide proof of valid software licensing upon request of the Contracting Officer, the NRC Project Officer, a Senior Information Technology Security Officer (SITSO), or the Designated Approving Authorities (DAAs).

The offeror shall ensure that its employees, in performance of the contract, receive Information Technology (IT) security training in their role at the offeror's expense. The offeror must provide the NRC written certification that training is complete, along with the title of the course and dates of training as a prerequisite to start of work on the contract.

The offeror must ensure that required refresher training is accomplished in accordance with the required frequency specifically associated with the IT security role.

Offerors shall ensure that their employees, consultants, and subcontractors that have significant IT responsibilities (e.g. IT administrators, developers, project leads) receive in-depth IT security training in their area of responsibility. This training is at the employer's expense.

The system shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The system shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators or system security officers and other security relevant events. The system shall be able to audit any override of security controls.

The offeror shall ensure auditing is implemented on the following:

- Operating System
- Application

- Web Server
- Web Services
- Network Devices
- Database
- Wireless

The offeror shall perform audit log reviews daily using automated analysis tools.

The offeror must log at least the following events on systems that process NRC information:

a. Audit all failures
b. Successful logon attempt
c. Failure of logon attempt
d. Permission Changes
e. Unsuccessful File Access
f. Creating users & objects
g. Deletion & modification of system files
h. Registry Key/Kernel changes
i. Startup & shutdown
j. Authentication
k. Authorization/permission granting
l. Actions by trusted users
m. Process invocation
n. Controlled access to data by individually authenticated user
o. Unsuccessful data access attempt
p. Data deletion
q. Data transfer
r. Application configuration change
s. Application of confidentiality or integrity labels to data
t. Override or modification of data labels or markings
u. Output to removable media
v. Output to a printer

The offeror shall ensure that backup media is created, encrypted (in accordance with information sensitivity) and verified to ensure that data can be retrieved and is restorable to NRC systems based on information sensitivity levels. Backups shall be executed to create readable media to which allows successful file/data restoration at the following frequencies:

- At least every 1 calendar day for a high sensitivity system
- At least every 1 calendar day for a moderate sensitivity system
- At lease every 7 calendar days for a low sensitivity system

The offeror must employ perimeter protection mechanisms, such as firewalls and routers, to deny all communications unless explicitly allowed by exception.

The offeror must deploy and monitor intrusion detection capability and have an always deployed and actively engaged security monitoring capability in place for systems placed in

operation for the NRC. Intrusion detection and monitoring reports will made available to the NRC upon request for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

The offeror shall work with the NRC project officer in performing Risk Assessment activities according to NRC policy, standards, and guidance. The offeror shall perform Risk Assessment activities that include analyzing how the architecture implements the NRC documented security policy for the system, assessing how management, operational, and technical security control features are planned or implemented and how the system interconnects to other systems or networks while maintaining security.

The offeror shall develop the system security plan (SSP) according to NRC policy, standards, and guidance to define the implementation of IT security controls necessary to meet both the functional assurance and security requirements. The offeror will ensure that all controls required to be implemented are documented in the SSP.

The offeror shall follow NRC policy, standards, and guidance for execution of the test procedures. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to NRC. The offeror shall include verification and validation to ensure that appropriate corrective action was taken on identified security weaknesses.

The offeror shall perform ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan, execution ST&E test cases and documentation of test results.

The offeror shall prepare the Plan of Action and Milestones (POA&M) based on the ST&E results.

The offeror shall provide a determination, in a written form agreed to by the NRC project officer and Computer Security Office, on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risked-based decisions. The offeror shall document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

The offeror shall develop and implement solutions that provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items.

The offeror shall perform verification of IT security weaknesses to ensure that all weaknesses identified through third party (e.g., OIG) audits are included in the POA&Ms that the quarterly reporting to OMB is accurate, and the reasons for any exceptions or risked-based decisions are reasonable and clearly documented. This verification process will be done in conjunction with the continuous monitoring activities.

The offeror shall create, update maintain all Certification and Accreditation (C&A) documentation in accordance with the following NRC Certification and Accreditation procedures and guidance:

- C&A Non-SGI Unclassified Systems

- C&A SGI Unclassified Systems
- C&A Classified Systems

Contract must develop contingency plan and ensure annual contingency testing is completed within one year of previous test and provide an updated security plan and test report according to NRC's policy and procedure.

The offeror must conduct annual security control testing according to NRC's policy and procedure and update POA&M, SSP, etc. to reflect any findings or changes to management, operational and technical controls.

C.5.2.2.7 Supplier Management

C.5.2.2.7.1 NRC Responsibilities

The NRC is responsible for relationships with suppliers other than those engaged by the offeror.

C.5.2.2.7.2 Offeror Responsibilities

The offeror shall develop and maintain excellent relationships with all sub-Contractors, suppliers and vendors so that the NRC can obtain high-quality services and equipment.

In addition, the offeror shall establish operating agreements with other service providers outside of their direct control.

C.5.2.3 Service Transition

Service transition relates to the delivery of services required by the business into live/operational use, and often encompasses the "project" side of IT rather than "BAU" (Business As Usual). This area also covers topics such as managing changes to the "BAU" environment.

Service Transition includes (among others) the topics of Asset and Configuration Management, Release and Deployment Management, and Change Management. Within the Service Transition area, the topics of Service Validation and Testing and Service Evaluation have been deliberately omitted. These topics deal with testing services carefully before they are provided and evaluating whether to proceed with a service. The processes are both somewhat simply descriptions of good business practices and do not warrant detailed description.

C.5.2.3.1 Transition Planning and Support

C.5.2.3.1.1 NRC Responsibilities

The NRC is responsible for approving service design packages, transition plans, and associated communications to the community of stakeholders. The NRC is also responsible for formulating reasonable release policies in collaboration with the offeror.

C.5.2.3.1.2 Offeror Responsibilities

The offeror is responsible for executing all other tasks and processes associated with Service Transition Planning and Support. Upon award of the ITISS contract, the offeror will describe a Transition Planning and Support approach that is substantially in alignment with the processes and procedures described in Section 4.1 of the ITIL v3 Service Transition publication.

C.5.2.3.2 Change Management

C.5.2.3.2.1 NRC Responsibilities

The NRC is responsible for formulating reasonable change policies in collaboration with the offeror; for chairing and appropriately staffing the Change Advisory Board; for furnishing appropriate rules for authorities to approve change to the offeror; and, for providing timely approval/rejection of changes. The NRC is also responsible for working with the offeror to keep the Change Calendar up to date with any impactful planned events that are initiated by the NRC.

C.5.2.3.2.2 Offeror Responsibilities

The offeror is responsible for executing all other tasks and processes associated with Change Management. Upon award of the ITISS contract, the offeror will describe a Change Management approach that is substantially in alignment with the processes and procedures described in Section 4.2 of the ITIL V.3 Service Transition publication. It is acceptable to describe that approach in a combined response to several of the Service Transition requirements in the SOW.

C.5.2.3.3 Service Asset and Configuration Management

C.5.2.3.3.1 NRC Responsibilities

The NRC has an obligation to its licensees and stakeholders for providing sound resource management. The Agency needs to have clear understanding of all of the IT assets in the infrastructure, in order to provide an appropriate level of transparency to those customers. Good configuration management, along with the knowledge of where each IT asset is and how it interacts with other IT assets in the infrastructure is also at the core of a good IT security strategy.

The NRC is responsible for furnishing the asset and configuration information that currently exists to the offeror for the purposes of the initial setup of the Configuration Management Database (CMDB). The offeror and the NRC must jointly agree on what the Configuration Items (CIs) will be and what relationships among CIs will be maintained in the CMDB. Primary responsibility for setup and maintenance of the CMDB and its integration into Change Management, Incident Management, Information Security Management, Problem Management as well as license management and other processes/functions resides with the offeror.

C.5.2.3.3.2 Offeror Responsibilities

The offeror shall identify, control, report, audit and verify configuration items supporting NRC services. The offeror shall account for configuration items throughout their lifecycle. For the purposes of this contract, a configuration item includes at least all versions of any authorized device or component that is managed by the ITI contract or that is attached to the network, and includes Government-furnished standalone laptop computers. This also includes, but is not limited to: firewalls, routers, hubs, switches, servers, printers, and all personal computing devices as well as software licenses residing on those devices. Secure and unsecure assets shall be combined in the CMDB.

The NRC recognizes that there is a great deal of complexity associated with this task. The agency seeks an offeror that has proven experience in developing and maintaining a comprehensive Configuration Management (CM) strategy. The NRC is focused more on the quality of the CM approach than on how rapidly it can be implemented.

The offeror shall provide, configure, populate, and manage a Configuration Management Database (CMDB) providing the foundation for many services and IT support processes associated with this contract. The CMDB will, at a minimum, identify all assets supporting NRC services with an appropriate level of starting detail. Initial detail shall include, at a minimum, unique identifiers, location, and description of the hardware or software with appropriate level of completeness. Appropriate linkages between key components and services need to be identified and implemented by the offeror. The offeror shall establish and enforce standard configurations (and images) that fulfill the business needs of NRC personnel and conform to security policies while recognizing that the workforce of the future expects a certain minimum level of technological sophistication. Verification and reporting shall be enforced by the offeror - automated discovery tools are quite mature and shall be utilized by the offeror to generate and ensure the accuracy of the basic asset list. The offeror shall utilize discovery tools to scan desktops weekly and report unapproved software on a monthly basis. The offeror shall provide a simple, cost effective process by which legitimate software can be considered for the approved list.

In addition, the offeror shall:

1. Protect the integrity of NRC assets per NRC security policies;
2. Be responsible for conducting a wall-to-wall or virtual inventory of applicable IT assets (both offeror-supplied and Government furnished), to be itemized for the NRC in an asset inventory; and,
3. Maintain the technical currency of hardware per original equipment manufacturer (OEM) standards, agreed-upon refresh schedules and NRC configuration standards.
4. Provide all adopted hardware standards to the NRC Enterprise Architect for incorporation into the NRC's Technical Reference Model (TRM).
5. Minimize the discrepancy between assets/inventory recorded in the CMDB and actual NRC assets/inventory. This includes ensuring minimally the following information for each unit:
    - Asset Tag
    - Serial Number
    - User Location (PCs and related peripherals only)
    - Configuration (OS, loaded software, etc)
    - Asset Status
    - Responsible Owner
    - Host Name (Servers only)
    - IP Address (Servers only)
    - Business Function/Application (Servers only)
    - Business Owner (Servers only)
    - Make/Model
    - Physical Location (Non-mobile units)

- Warranty Info / Maintenance Certificate Number (Servers only)

Software License Management – The offeror shall manage workstation, server, and network component operating systems and software licenses and license keys. The offeror shall ensure that NRC hardware and software components are within license requirements.

In addition, the offeror shall:

1. Create and maintain a database of workstation software, server software, server operating systems and patch level, and operating systems;
2. Provide metrics on license usage including number of licenses owned but not in use, and products not adequately licensed. There will be monthly reviews of these reports with the NRC to help define problems or needs for software removal or license purchases;
3. Verify assets on a periodic basis for the purposes of asset management and license management; and,
4. Provides all management, hardware and software supporting the above mentioned databases and the management processes for those databases.
5. Provide all adopted software standards to the NRC Enterprise Architect for incorporation into the NRC's Technical Reference Model (TRM).

Vendors shall describe a "best value" CMDB approach that balances complexity and cost of maintenance with utility to the NRC and the offeror.

C.5.2.3.4 Release and Deployment Management

C.5.2.3.4.1 NRC Responsibilities

The NRC is responsible for approving deployments and approving the associated communications to stakeholders. The NRC is also responsible for providing appropriate authorized personnel throughout the release and deployment process to make go/no go and back-out decisions promptly.

C.5.2.3.4.2 Offeror Responsibilities

The offeror is responsible for executing all other tasks and processes associated with Release and Deployment Management. Upon award of the ITISS contract, the offeror will describe a Release and Deployment Management approach that is substantially in alignment with the processes and procedures described in Section 4.4 of the ITIL v3 Service Transition publication. The offeror shall provide and manage appropriate tools to manage the overall transition process.

C.5.2.3.5 Knowledge Management

C.5.2.3.5.1 NRC Responsibilities

The NRC is responsible for furnishing existing knowledge to the offeror in bulk at the beginning of the contract and as requested thereafter. The NRC is also responsible for attending quarterly meetings led by the offeror to analyze data, synthesize information based on that data, identify any knowledge gaps that exist, and help to fill those gaps. Furthermore, the NRC is responsible for identifying rules concerning what functional roles should have access to what knowledge.

C.5.2.3.5.2 Offeror Responsibilities

The offeror shall provide and maintain a document repository accessible by all support staff and select NRC staff of processes, procedures, and technical manuals. A subset of information shall be available for users to search and resolve minor incidents. In addition to this document repository, there is a need for a knowledge management and dissemination approach that balances reasonability and ease of maintenance with the obvious benefits of having the right training, communications, and historical knowledge in the hands of offeror and NRC staff when they are needed. The NRC is aware that over-engineered Knowledge Management efforts frequently sacrifice the "good enough" to the quest for perfection and can become costly failures as a result. Vendors shall suggest reasonable knowledge management processes, procedures, and technologies that have been proven to work at other clients. Information already included in the service desk description need not be repeated in response to this section.

The offeror will be responsible for maintaining the original versions of documents.

In addition, the offeror shall maximize the availability of the document repository (containing processes, procedures, technical manuals, and other relevant documentation in support of NRC services)

C.5.2.4 Service Operation

Service Operation is the business of achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the SLAs). Service Operation is the part of the lifecycle where the services and value are directly delivered. Service Operation also includes monitoring problems and considers the balance between service reliability and cost. Topics include balancing conflicting goals (e.g. reliability vs. cost, etc.). This section also includes a discussion of the service desk Function, which spans a great deal of the Service Operation topics.

C.5.2.4.1 The Service Desk Function

The current service desk implementation includes multiple service desks at headquarters (Agency-wide Documents Access and Management System - ADAMS, Time and Labor, Enterprise Project Management - EPM, etc.) as well as Local service desks within the regions. There is also not a central shared ticketing system, although Magic (now a BMC tool) is utilized by some desks. The user experience today is primarily as follows:

- The user dials "1234" on their telephone and reaches an automated voice system asking if their topic is ADAMS, HRMS, EPM, etc.;
- Once the user selects their choice, a recorded message concerning any known problems is played if appropriate. The user is then put through to support personnel who begin a ticket;
- If the user unwittingly picked the wrong choice, they are transferred to another individual;
- If the Help Desk Level 1 support cannot answer the question, the user's ticket is recorded and forwarded to Level 2 support for resolution; and;
- Escalation is not always done according to crisp rules.

In general, service desk support utilizes a modified 15 x 7 dedicated support plus on-call hours of operation model, with 15 x 5 Monday through Friday and 12 x 2 on weekends. All other hours are on call for Chairman and Commission staff (approximately 40 users). A predominant number of the Local service desk staff are budgeted by, and paid for by the regions and are not managed by or coordinated through the Centralized service desk.

IT Coordinators serve as the liaisons between each NRC Office and the Network Operations and Customer Service Branch (NOCSB). IT Coordinators must approve requests for network access and access to server-based applications, remote access, software installation, moves or removals of desktops, software or peripherals acquisitions, and desktop upgrades. IT Coordinator responsibilities include:

1. Email and coordinate user requests to the Customer Support Team;
2. Approve and submit Electronic Move Requests for all microcomputer equipment moves and network account moves;
3. In some cases, procure non-infrastructure hardware and software using the NRC Bankcard program if a Bankcard holder;
4. Communicate changes in IT Coordinator personnel to the Office of Information Services;
5. Attend OIS briefings on IT issues Serve as Office liaison between office staff and the OIS to coordinate Agency-wide software upgrades; and,
6. Inform the OIS about any changes to the office computing environment.

To the extent possible, the NRC would like to consolidate service desk functions at headquarters into a single centralized service desk with shared ticketing, procedures, and specialized support at Tier 2 (one of the service desks is currently outsourced to a third-party vendor and may not lend itself to consolidation). The NRC wishes to share resources, tools, and procedures between the Central and Regional service desks. Because of the sensitive nature of some of the information handled by the NRC, off-shoring this function is not a viable solution. There is not a requirement for service desk staff to be co-located with NRC staff beyond the need to maintain sufficient staff at local sites for providing deskside support. Local staff may report to and be dispatched by the centralized service desk. If the offeror proposes an off-site Help Desk, they must also propose a viable, federally-approved, secure mechanism for remote access to user workstations for providing support.

The offeror shall balance the staff skills and levels of staffing to address the service level requirements found in Appendix A: *SM-SLA-11: Service Desk*. The offeror shall manage and enforce policies and procedures across all service desk staff. Dedicated offeror staff shall be available business weekdays 6:00 a.m. to 9:00 p.m., weekends 9:00 a.m. to 9:00 p.m. EST, and on-call services available at all other times, including all holidays. Procedures and tools shall be established by the offeror to increase resolution of incidents and fulfillment of request at Level 1.

The offeror shall collect, review, and provide metrics to validate appropriate staffing levels and adjust as needed. Procedures and SLRs for on-call response times need to be documented by the offeror and agreed upon by the NRC, including "special circumstances processes" to invoke immediate response when required. Clear communications of current known incidents and known problems and workarounds shall also be provided by the offeror. A knowledge database with "known fixes" shall be implemented by the offeror.

The offeror shall make self-help tools, including password reset, available to NRC users. It is essential that these self-help tools address all NRC and Federal security policy.

The offeror shall provide standard industry software to accept, manage, and resolve user incidents. The offeror shall provide access to this software to appropriate NRC staff members. The tool shall have the capability to provide self-service submission of incidents as well as the ability for the user to check status on any open ticket. Technology should be leveraged to allow service desk staff to take control of a remote computer to troubleshoot/repair issues.

The offeror shall recommend an approach for NRC approval in each of the following areas:

1. Three-tier incident severity ratings shall be established with clear criteria;
2. Escalation procedures and criteria shall be established;
3. Training programs for new service desk personnel shall be described; and
4. Knowledge Base for continuous improvement shall be established.

The offeror shall describe a cost-effective approach to providing an integrated, highly-effective service desk function that receives acceptable customer service ratings. The offeror shall provide real examples from existing customers including customer service ratings and customer contact information.

In addition, the offeror shall:

1. Report all verified or suspected computer security and/or unauthorized PII release incidents immediately to the NRC CSIRT;
2. Minimize the time from when a phone call enters the Service Desk queue to when a live agent takes the call and works with the user;
3. Maximize the number of calls/contacts that are reasonably resolved upon "first contact" (i.e. resolved without warranting additional calls to the Service Desk)
4. Minimize the number of Service Desk calls that are disconnected (abandoned) before reaching a live agent;
5. Minimize the time in which a user is on hold, prior to either reaching a live agent or abandonment;
6. Minimize the percentage of tickets that need to be reopened to complete resolution;
7. Minimize the time from when an e-mailed request for assistance is sent to when the service desk responds to the request;
8. Minimize the time from when request for assistance is sent through the web portal to when the service desk responds to the request;
9. Maximize the number of incidents that are correctly escalated;
10. Maximize the availability of live agents and of customer-facing applications (e.g. Customer Service Portal); and,
11. Maximize customer satisfaction.

C.5.2.4.2 Event Management

C.5.2.4.2.1 NRC Responsibilities

The NRC is responsible for setting thresholds with the offeror defining what constitutes an event and for revisiting these thresholds periodically.

C.5.2.4.2.2 Offeror Responsibilities

In addition to responsibilities described in Section *C.5.2.4.1 The Service Desk Function*, the offeror will be responsible for Event Correlation and for integration of the monitoring software into the Incident Management software as described in Section *C.5.2.4.3 Incident Management*.

In addition, the offeror shall:

1. Provide all tools associated with managing and responding to NRC ITI events.
2. Maximize availability of ITI service
3. Minimize the time from the identification of any failure, to the notification of the appropriate Agency personnel

C.5.2.4.3 Incident Management

C.5.2.4.3.1 NRC Responsibilities

The NRC is responsible for setting the escalation and incident severity rating scales with the offeror, and for the review of incidents to identify problems with the offeror. The NRC is also responsible for providing Level 2 support for the resolution incidents for certain applications:

Large Scale Applications – Applications which effect a large number of users (including users external to the NRC and/or applications which are critical to the agency's mission:

Name	Description
Administrative Services Request System	Web portal which gives access to NRC administrative services (Visitor Access, Maintenance Fixes, etc.) – Opens links to other Web-based applications
Digital Data Management System	Adjudication hearing management support system, including management and storage of all documents (in electronic form) used to manage cases
Financial Accounting and Integrated Management Information System (FAIMIS)	Integrated financial management tool that incorporates billing, cost accounting, budget execution, and capital property management
Time and Labor	Timekeeping tool for NRC employees to report and track their time.
General License Tracking System	Tracks transfers and disposition of devices containing potentially hazardous nuclear materials.

National Source Tracking System	Tracks nuclear devices and sources from their manufacture, through their "life-cycle" of transfer to and ownership by licensees, including their eventual disposal at authorized facilities
Web Based Licensing License Tracking System	Tracks material licensee applications for use of byproduct, source, and special nuclear materials
High-Level Waste Collection System	Repository of publicly collected documents extracted from ADAMS pertaining to the High Level Waste Facility at Yucca Mountain
Electronic Hearing Docket System	Enables authorized participants to submit and retrieve documents electronically and supports public access to publicly available documents online
Enterprise Project Management	Scheduling, collaboration and workload management tool using Microsoft Enterprise Project and Microsoft SharePoint
Emergency Response Data System	Provides plant condition data from nuclear plants to allow the NRC to monitoring licensees during an incident and assure that appropriate recommendations are being made
Agencywide Document Access and Management System	Document and records management tool to store agency Official Records
Electronic Information Exchange System	Web-based portal that allows external entities to transmit data and files electronically to the NRC

Moderate Scale Applications – Applications that effect external entities but are utilized by only a small group of NRC users and/or applications that have high internal political interest but are not mission-critical:

Name	Description
EDO Document and Action Tracking System (EDATS)	Agencywide system to track assignments that are made across offices or from the Commission to offices
Reciprocity Tracking System	Track Agreement State licensee requests for reciprocity
Terminated License Tracking System	Tracks NRC terminated material license sites
Strategic Workforce Planning	Tracks NRC employee core competencies and skills and allows compares with skill requirements
Protected WEB Server	Used for sharing non-safeguards but sensitive information with licensees
Individual Action Tracking System	Tracks enforcement actions against individuals
FOIAXpress	Tracks FOIA requests and responses

Public Meeting Notice System	Supplies NRC public meeting information to the public
Funds Execution System	Tracking and monitoring the use of contract, travel, and training funds at the project level
NRC Knowledge Management Center	Collection of expert knowledge based on lessons learned and best practices
Electronic Library	Collection of electronic documents used to assist Incident Response teams providing detailed up-to-date information

Small Scale Applications – Applications that only effect a small group of users and are not mission-critical:

Name	Description
Commission EDO/IG Budget Tracking System	Tracks program support, travel, awards, and change of station
Nuclear Regulatory Commission Report Processing System	Document generation program that formats NRC regulations
Space Property Management System	Archibus and Autocad system used to plan and manage NRC building and office space
EDO Label System	Office efficiency system used by EDO to produce sequentially numbered labels which identify and track written communications with the EDO office
SES Succession Planning System	Web application for SES succession planning
OGC Legal Memoranda File	Provides access to working copies of legal reference documents by OGC staff
Office of the Inspector General Management Information System	Manages audits and investigations conducted by OIG
OIG Travel System	Office tracking system used by OIG to track travel authorizations, advances, obligations and expenditures
Voyager Integrated Library System	Used for acquisitions and funds management, cataloging, circulation, series control, and an online public access catalog in the NRC Technical Library
Archival Facility Activity System	Contains all records transfer and accountability information for NRC's official records retired to the NRC Archival Facility and the National Archives and Records Administration
SECY Tracking Reporting System	Tracks Commissioners' documents, votes, and meetings
Record Classification Actions System	Tracks classification and declassification of NRC records, which relate to national security information & material.

Currently, there are not clear procedures in existence for how incidents are escalated from the help desk to the NRC, especially for unexpected incidents. In their proposal, the offeror shall make general recommendations for incident escalation procedures. Upon award, the offeror shall perform an assessment of NRC incident escalation and make recommendations

for when and how incidents will be escalated. Once approved by the NRC, these procedures shall be followed by the offeror when incidents need to be escalated to the NRC.

C.5.2.4.3.2 Offeror Responsibilities

The offeror is required to:

1. Troubleshoot and resolve incidents and problems from a total systems perspective including desktop, software, networking incidents, etc.;
2. Document and track all incoming incidents and provide analysis for those incidents;
3. Support end-users at the NRC headquarters by responding directly to end-users requests for help and responding to calls from designated NRC staff and technical support staff;
4. Support remote and mobile users by responding directly to end-users requests for help and responding to calls from designated Regional IT staff and Headquarters IT staff;
5. Provide a single, integrated service desk for all NRC ITI incidents and service requests;
6. Delineate and manage customer needs and expectations;
7. Prioritize service requests according to severity;
8. Prioritize incidents according to severity;
9. Provide service desk support for Agency office productivity suite (Currently MS Office 2003) and also provide support for other specific software that is not part of the standard image;
10. Provide application support services for infrastructure systems such as MS SharePoint and MS Outlook;
11. Provide custom reports when requested by the NRC using information from the ticket tracking system;
12. Document the steps that were taken to resolve incidents;
13. Resolve incidents on the first call where possible, or dispatch staff to correct problems, in person, as necessary;
14. Recommend an escalation procedure for handling bursts of incidents and implement that procedure when requested by the NRC;
15. Provide workstation virus removal; resolve connectivity issues; and resolve other types of failures that result in the inability of one or more end users to utilize the computer to perform job functions;
16. Provide support and on-site maintenance for offices (Office of the Commission [OCM], Office of the Inspector General [OIG]) where desktop systems must remain with the office unless directed otherwise by the NRC;
17. Minimize the time from the initiation of a Service Desk incident, to the time in which the service is restored; and,

18. Minimize the discrepancy between recorded incidents and actual incidents.

C.5.2.4.4 Problem Management

C.5.2.4.4.1 NRC Responsibilities

The NRC will advise on the priority in which problems should be addressed and provide policy as to the definition and management of problems.

C.5.2.4.4.2 Offeror Responsibilities

The offeror is responsible for problem management. The offeror shall propose a problem management approach and implement that approach when approved and requested by the NRC. The offeror shall establish a Known Error Database (KEDB) to record known errors, their resolution and workarounds. Views of the KEDB shall be made available by the offeror to end user for the purposes of self service.

In addition, the offeror shall minimize the time between the identification of a problem and the resolution of that problem by identifying a suitable workaround and/or permanent solution.

The offeror is responsible for the identification of the root cause of problems and the development of an implementation plan. Upon approval of the NRC, the offeror shall remediate the underlying problem based on established release and change management processes and procedures.

C.5.2.4.5 Request Fulfillment

C.5.2.4.5.1 NRC Responsibilities

The offeror is primarily responsible for Request Fulfillment. The NRC is responsible for determining what requests would trigger the development of new services.

C.5.2.4.5.2 Offeror Responsibilities

The offeror shall resolve all service requests placed to the service desk.

In addition, the offeror shall:

1. Assist in the development of procedures for the consistent handling of service Catalog offerings;
2. Identify service requests that are not currently covered by the service Catalog, and present them to the NRC for consideration in the development of new services;
3. Provide for self-service password reset that meets NRC IT security requirements;
4. To the greatest extent possible, provide other automated request fulfillment capabilities; and,
5. Minimize the time between the initiation and fulfillment of a service request.

C.5.2.4.6 Access Management (and the Directory)

C.5.2.4.6.1 NRC Responsibilities

The NRC currently has an Active Directory implementation. By the time the new ITISS contract is let, it is anticipated that Novell Directory Server (NDS) will have been removed from the environment. Going forward, the NRC would like a more robust directory

implementation. The NRC is responsible to furnish the information required to develop and maintain the directory.

C.5.2.4.6.2 Offeror Responsibilities

The NRC requires a directory service for locating, managing, administering, and organizing common items such as network resources, folders, files, printers, users, groups, devices, telephone numbers and other objects.

The offeror shall plan, develop, manage and improve upon an accurate, current, and automated organizational hierarchy of users, devices, domains and other resources. The offeror shall also propose ways to leverage the directory to automatically produce organization charts and other useful artifacts.

In addition, the offeror shall manage, maintain, administer, and support the NRC's Address and Domain Services to provide IP address management and domain services including but not limited to the Windows Domain and Domain Name Services (nrc.gov, usnrc.gov, nrc-gateway.gov and sub-domains).

The offeror shall utilize the Directory to help identify users, ensure appropriate access to services, and assign policies.

In addition, the offeror shall:

1. Provide a central directory for which access rights are granted based on roles;
2. Provide management and maintenance of user access controls for data files, directories, and volume access;
3. Manage user and group profiles to manage roles containing one to multiple users;
4. Support, revise, and implement system safeguards such as directory structures, access controls, and procedures;
5. Provide a report of the resources to which any user has access;
6. Provide a report of all users that have access to any given resource;
7. Support and manage Personal Identity Verification (PIV)-2 compatible equipment on personal computing devices;
8. Support PIV-2 logical access to NRC ITI resources;
9. Make the Directory available to any existing or future business applications that wish to use it for authentication;
10. Support the integration of the Directory with Agency applications to reduce the number of passwords users need while maintaining or improving the level of operational IT security. This would include reduced sign-on via PKI or PIV card;
11. Authenticate users to all resources under the control of the offeror;
12. Ensure that any new applications introduced by the offeror as part of maintaining the infrastructure use the Directory for access and authentication;
13. Provide an automated self-help password reset function based on security questions to be determined in accordance with the NRC security requirements;
14. Maximize the availability of the LDAP service;

15. Minimize the time between the request for, and delivery of, an access management request (e.g., requests to create, update, maintain, or disable accounts; requests to alter the security profile rights for control groups or distribution lists; etc.); and,
16. Minimize the time between the request for, and fulfillment of, valid password reset requests.

C.5.2.4.7 Other Service Operation Considerations

The NRC regularly adds and changes technologies in the NRC ITI. However, as existing IT services are vital to the day-to-day productivity of NRC users, it is essential that the introduction of these changes does not disrupt normal Agency operations.

Therefore, all modifications to the NRC ITI must be thoroughly tested in the Agency's test environment and appropriate precautions must be taken to mitigate any disruptions that they might introduce. This test environment must appropriately replicate the actual production environment so that the tests can be as accurate as possible and real problems can be identified and corrected. Although individual IT system owners must take the responsibility to move their systems through this process, the offeror shall help them to succeed in this endeavor.

The offeror shall propose a risk management approach that includes a set of Key Risk Indicators and a risk management and measurement plan. Examples of Key Risk Indicators might include (the NRC is providing these as examples, not guidance or requirement):

- Turnover rate of personnel managing critical systems
- Critical system downtime due to environmental disruption
- Critical system downtime due to IT security breaches
- Critical system downtime due to IT change
- Number of planned IT changes at different levels of severity
- Time between gap closures
- Risk of maintaining the status quo

The offeror shall also perform all database activities described in the optional task in Section C.6.3.4.2 Database Support for all databases related to the Core and any Optional Services.

C.5.2.5 Continual Service Improvement (CSI)

All NRC employees require timely, reliable, and accurate information in order to make decisions. Shared information about the NRC ITI, ongoing project schedules, security incidents, emerging trends, external suppliers, incident status, and accomplishments help to build trust and allow for a shared ownership in successes and failures alike.

In addition to the reporting described below, the offeror and the NRC will meet quarterly to review at least one new area selected by the NRC for Service Improvement to develop a plan for improvement and to review results in ongoing improvement plans. The NRC will agree with the offeror on the area for improvement no later than the third week of the quarter.

The offeror shall review solutions and improvements that they have implemented for other customers and make recommendations for how similar improvements could be made at the NRC. If approved by the NRC, the offeror shall implement these improvements.

Vendors are free to propose other programs for Continual Service Improvement (CSI).

C.5.2.5.1 Centralized Reporting

The offeror shall provide a dashboard which provides the ability to review a high level status of all report deliverables under this contract. The dashboard shall provide the capability to "drill down" to underlying data. All NRC users will be provided access to the dashboard and some of the underlying data. Select NRC users will have access to all underlying data.

C.5.2.5.2 Proactive Reporting

The offeror shall notify ITI users well in advance of scheduled outages.

In addition, the offeror shall provide daily status reports describing any insufficiencies, expected or unexpected outages, or unusual incidents by 7:00 a.m. (Eastern) for the past 30 hours, including weekends.

C.5.2.5.3 General Reporting

The offeror shall generate and deliver standard as well as custom-designed and ad hoc reports at both a summary level and various detail levels about the NRC ITI. The offeror shall develop and deliver technical and managerial oversight status presentations to NRC management. See section *Appendix E: Reporting Requirements* for a greater understanding of NRC's general reporting requirements.

In addition, the offeror shall:

1. Provide a Monthly Status Report covering all contract activity of the previous month;
2. Provide user access reports defining who accessed resources and when;
3. Provide user access reports defining who has been granted access to resources;
4. Provide network management reports as requested by the NRC Project Officer, such as Network Performance and Availability reports, System Utilization reports, application response and utilization, Network device Identity, IP address and Network Growth reports;
5. Provide monthly disk space and capacity reports;
6. Provide a bi-weekly report on mailbox caps and exceptions;
7. Recommend, and provide reports based on industry best practices in service desk management;
8. Report the number of calls closed on initial contact;
9. Report the average speed of answer, the abandon rate, the number of incidents reopened, and the number of calls handed off to a second tier;
10. Reports the number of requests for repair/maintenance of trouble calls processed and their current disposition;
11. Provide periodic inventory reports and various organizational or inventory account reports;

12. Report the number of requests for property and property control forms processed;
13. Report of equipment totals with the following status information: number received, number distributed, number excessed, and the number in stock;
14. Report notification for procurement of equipment to refresh stock or renewal of maintenance, the status of existing on-hand hardware and or service plans;
15. Provide monthly software usage and compliance reports, identifying any discrepancies;
16. Provide a monthly Security Summary Report;
17. Provide and maintain an updated list of project deliverables with completed or scheduled delivery dates;
18. Provide reporting that shows all desktop, peripheral, and or infrastructure component failures during a specific time period; and,
19. Provide outage reporting that shows the duration of any downtime and the services impacted.

C.6 OPTIONAL SERVICES

C.6.1 Computer Facilities Management

This section describes the specific requirements, using the NRC ITISS contract vehicle, for managing the Agency's computer facilities and computer application server hardware and software in support of the Agency's mission.

C.6.1.1 Program Management

The offeror's Program Manager shall meet with the NRC Project Officer to review the status of ongoing efforts and to discuss other work projects planned or proposed. The offeror shall be responsible for maintaining day-to-day operations of each computer facility and shall provide coverage for the NRC computer facilities 24 hours a day, 365 days per year. The offeror shall perform all required day-to-day operational activities including system operations and maintenance of the hardware, software and application systems and perform backup and recovery of systems as well as monitor all systems and the computer facilities environment.

In addition, the offeror shall:

1. Provide on-call support in addition to the support required during the scheduled hours; and,
2. On-call personnel shall arrive at the appropriate computer facility within one hour after notification by the Project Officer. On call personnel will be able to perform or contact someone to perform any task that can be performed during regular hours. If the offeror's designated personnel are unable to arrive at the NRC site within one hour, they shall notify the Project Officer and request approval for the delay.

C.6.1.2 Monitoring

The offeror shall monitor the computer facility environment including air conditioning, humidity, and power distribution. All system activities shall be monitored on a continuous basis with appropriate documentation of activities, problems, equipment failure, and other logging to record irregularities in normal facility operations.

Additionally, the offeror shall:

1. Ensure all processes are running and all remote communication links are up;
2. Conduct systems checks in all computer facilities on agreed upon schedule;
3. Check for and properly distribute printed output (The NRC utilizes the DOI personnel system and mainframe computers at the NIH. Periodically, printouts are sent directly to NRC printers. The offeror will be provided with a distribution list to determine how to properly distribute these printouts based on their type); and,
4. Through continuous monitoring, ensure system availability for all systems; if unavailable, notify system owners or specified points of contact to return systems to operational state.

C.6.1.3 Quality Assurance

The offeror shall develop, write and maintain quality assurance procedures for all computer facilities activities. The offeror shall also maintain and document production installation

information, troubleshooting techniques, problems encountered, configuration information and default settings. Systems and procedural documentation shall feed the Configuration management system and be updated within 24 hours of any change.

The offeror shall also implement a risk management strategy as described in the Service Operation section of this document.

The NRC will review these procedures and strategies and recommend any modifications prior to approval. Once approved, the offeror shall comply with these procedures.

C.6.1.4 Backup and Recovery

The offeror shall perform backup and recovery services for all systems in the computer facility with the backup level of service. Backup shall be performed on established schedules.

In addition, the offeror shall:

1. Provide backup data as required;
2. Performs systems backup following established schedules;
3. Maintain clean, quality backups that are encrypted;
4. Replace backup information for HRMS as needed and notify HRMS systems staff regarding problems;
5. Prepare backup data for off-site delivery;
6. Enter backup data from off-site delivery into library database;
7. Perform backup data library tasks as required including entering information into the library database;
8. If using tapes, prepare scratch tapes, clean and degauss tapes;
9. Label and retain backup of real event data until all investigations are completed and data is released for distribution or reuse;
10. Ensure that all data is in a state of readiness. If using tape, only clean, certified tapes shall be issued to users. Any tapes not meeting the Governments minimum certification requirements shall be degaussed and discarded;
11. If using tapes, maintain a log that indicates reasons for all tapes discarded as well as a count of the tapes provided to the Project Officer in a weekly report;
12. Perform incremental and full backups based on established guidelines;
13. Facilitate the flow of backup data to and from other contract services and prepare all data shipping forms; and,
14. Assist the Project Officer in conducting a semi-annual verification of backup data logs.

C.6.1.5 Computer Operations

The offeror shall operate all computers, remote job entry stations, related support equipment and communications equipment in the computer facilities. The offeror shall also perform regular operations and preventive maintenance on equipment.

In addition, the offeror shall:

1. Manage periodic equipment replacement and the development of new server configurations;
2. Maintain activity, problem, equipment failure, or other logs to record irregularities in normal facility operations;
3. Provide user support or contacts for related problems;
4. Maintain communications with hardware vendors regarding problems or maintenance;
5. Interface with the customer support center, systems administration staff and specified ADAMS points of contact regarding ADAMS availability;
6. Assist users with job procedures and standards, resolution of operations related problems and delivery of computer facilities products;
7. Inform individuals contacted of the system problem, causes and estimated time of recovery, if known;
8. Report all system hardware and software problems, air conditioning malfunctions, power supply failures, and humidity control problems immediately to the Project Officers of the maintenance Contractor or designee; and,
9. Maintain logs; enter detailed information into the appropriate log on a daily basis.

C.6.1.6 Physical Facility

The offeror shall maintain the physical facility in relation to security and general housekeeping. This includes putting trash in trash cans, discarding paper in recycling bins, discarding sensitive printouts in burn bags and other generalized house keeping.

The offeror shall control physical access to each computer facility, admitting only those persons for whom access has been approved by the computer facilities information security officer. The offeror shall report security related events to the computer facilities information systems security officer in accordance with the NRC incident response policy upon discovery of the incident.

In addition, the offeror shall:

1. Remain in the computer facilities during pre-scheduled preventive maintenance, emergency maintenance, and workers other than access approved staff is performing any services in the computer facilities; and,
2. Ensure the appropriate level of security controls are implemented and/or maintained.

C.6.1.7 Specialized Systems

C.6.1.7.1 Agency-wide Documents Access Management System (ADAMS)

ADAMS is a computer-based document storage and retrieval application that serves as the NRC's official record-keeping system. This application permits the NRC staff to search for letters and memoranda and other types of correspondence issued by the NRC and events dealing with any NRC licensed users of nuclear energy. This system is critical to the operation of the Agency and shall be updated daily with the latest records. This system is based around IBM FileNet software with an NRC custom application. However, this system

is currently being migrated to IBM Panagon P8 and will rely much more on commercial off-the-shelf software with many fewer NRC customizations. All requirements for ADAMS apply also to the successor system (referred to as Enterprise Content Management).

In addition, the offeror shall:

1. Monitor ADAMS to maximize the availability of the application to the users. In the event there is a problem, the offeror shall notify the appropriate support staff;
2. Post the daily transactions, full text data (when necessary), perform daily backups, and ensure data synchronization to backup site was successful;
3. Assist in the verification process by providing reports, record counts, or other information to the support staff; and,
4. Be responsible for the generation of scheduled reports and backup data and facilitate the transmittal of backup data to off-site storage facility.

C.6.1.7.2 Human Resource Management System

The HRMS application provides a single application for the processing of the NRC's time and labor records. The offeror shall ensure that the system is running and assist with any troubleshooting activities if a problem is encountered during the bi-weekly processing of this application in support of the NRC's Task Managers.

In addition, the offeror shall:

1. Submit and monitor various production jobs according to the processing schedule;
2. Generate and provide to other contractors data for various off-site processing. If using tapes, these tapes shall be labeled and tracked in the tape management system;
3. Incorporate any modification to the payroll processing schedule into the monthly work schedule as notified by the NRC task managers;
4. Assist users with job procedures and standards, resolution of operations related problems and delivery of computer facilities products;
5. Attend meetings to assist in the development of implementation plans for proposed changes in the operations of applications (assume 2 meetings annually);
6. Maximize the availability of the resources within the NRC Data Center;
7. Minimize the discrepancy between date of scheduled system backup and date on which the system backup occurs; and,
8. Maximize the availability of agency-specific applications, including
    a. Emergency Response Data System (ERDS)
    b. Agencywide Documents Access and Management System (ADAMS)
    c. Enterprise Project Management (EPM)
    d. Time and Labor

C.6.2 Operations Center Network Management

This section describes the specific requirements, using the NRC ITISS contract vehicle, for managing the Agency's Headquarters Operations Center network and information management system in order for the operations center staff to continuously receive and document notifications from licensees and others to ensure that the public is adequately protected.

Personnel supporting the Operations Center must possess an "L" security clearance that allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data.

C.6.2.1 Operations

The Headquarters Operations Center is responsible for managing information pertaining to the daily operational status of nuclear facilities and nuclear events. The primary system for managing the information is the Operations Center Information Management System (OCIMS). OCIMS supports NRC's vital role of providing leadership focus for national and international information distribution and decision support. OCIMS is composed of several information systems which include the operations center network infrastructure, personal computers and servers, systems that support response operations (WebEOC which is a crisis information management system) and the Headquarters Operations Officer System (HOO) , Private Branch Exchange (PBX) and associated telephones, teleconferencing system, voice recording system, other communications hardware, audio video display system, and personal computer peripheral equipment. The offeror shall provide all labor supervision, tools, materials, parts equipment and transportation necessary to manage and administer the Operation Center information management system network and hardware and software maintenance of the OCIMS.

In addition, the offeror shall:

1. Be responsible for the operation of the systems, providing LAN administration, hardware and software maintenance services **on-site** during the principal period of maintenance (PPM). During the PPM, there will be two offeror employees on-site in the Operations Center and will be required to maintain an L level security clearance. The PPM is defined as 7:30 a.m. to 6:00 p.m. (EST), Monday –Friday excluding Government holidays;
2. Provide the same services on an on-call basis at times outside the PPM and response times are as follows: telephone within 1 hour; onsite within 2 hours;
3. Respond to the Operations center whenever NRC activates its incident response function to keep all of the OCIMS systems operating as well as providing hardware/software troubleshooting when failures arise, and have the capability to provide one staff person on-site 24 hours per day for up to 30 days after notification by the NRC Project Officer;
4. Perform WebEOC event archives and event clean up after each use;
5. Administer the OCIMS local area network (LAN) including network switches, server connectivity, user administration, network security, etc;
6. Maintain and update/revise the OCIMS documentation in both hard copy and electronic formats including the standard operating procedures (SOP), hardware and software lists, and other documentation as required by the NRC Project Manager;

7. Maintain and update/revise the other documentation in both hard copy and electronic formats: Onsite Maintenance Logs, 3rd party manuals, as-is documentation, and Federal Information Security Management Act (FISMA) documentation;
8. Maintain the OCIMS hardware and software inventories. Shall use the Agency's property inventory system (read only rights) to maintain the hardware in conjunction with the NSIR Operations Center IT Coordinator.
9. Follow all guidance provided in NRC Management Directive 2.1 as it concerns the documentation of all information technology;
10. Make routine and ad hoc preventive and correct changes to the OCIMS databases as requested or approved by the NRC Project Officer;
11. Coordinate with NRC staff and other contractors to resolve issues that may arise related to Government provided resources that support OCIMS;
12. Maintain maintenance agreements with vendors who support the following equipment: PBX, conferencing system, voice recording system, audio/visual display system, UPS, satellite and dish network, software maintenance agreements (ESRI, Impact Weather, WebEOC, etc.), printers and scanners;
13. The offeror shall implement system backup and restore procedures to ensure that OCIMS is maintained with complete backup and have the ability to be restored.
    - In addition the offeror shall:
        - Perform a daily, weekly and monthly backups of OCIMS as specified in the SOP for the backup system;
        - Enhance and/or modify the backup and recovery programs as needed (with prior approval of NRC Project Officer);
        - Maintain up to date backup data inventory, per the SOP.
    - Maintain continuity of operations (COOP) capabilities.
14. Maintain required certification and accreditation for the OCIMS system (perform quarterly scans, maintain patch levels and other Computer Security Officer (CSO) requirements;
15. Maximize the availability of the NSIR Operations Center (i.e. minimize the length and frequency of service outages); and,
16. Minimize the time between the notification of, and response to, an incident.

C.6.2.2 Hardware Maintenance

The offeror shall perform day to day operations and maintenance and on-site technical support of OCIMS as well as provide preventive maintenance on various OCIMS equipment and keep the equipment in operating condition consistent with best practices. Currently, most of this hardware is owned by the NRC. The offeror shall recommend a strategy for the replacement of OCIMS hardware with offeror-supplied hardware over a period of time as the current hardware comes to the end of its refresh cycle. The offeror shall also be required to update the OCIMS asset inventory list when additions and/or deletions are made in the OCIMS environment.

C.6.2.3 Software Maintenance

The offeror shall provide software maintenance to include upgrades of non-Agency standard software. The offeror shall also be required to update the OCIMS software list when additions and/or deletions are made the OCIMS environment.

In addition, the offeror shall:

1. Maintain the operating system, currently MS Server, and user database (Active Directory). Maintain primary and backup domain servers, print servers, and DNS servers.
2. Maintain the database management software (currently Sybase ASE v12 and MS SQL) for both WebEOC, HOOs, and GIS, which includes backup, restoration, and table maintenance;
3. Maintain WebEOC and HOOs software and review applications once per month and prepare user comments and concerns to determine if changes are needed to support the incident response function;
4. Work with other contractors who provide additional Operations Center software (e.g., ERDS, RASCAL, etc.)
5. Provide on-site support during the PPM and telephone support at other times; and,
6. Respond to special orders for services outside of the PPM for providing troubleshooting assistance via telephone to the on-site Government staff so as to facilitate repairs upon arrival.

C.6.2.4 Reporting

The offeror shall provide a weekly status report and a monthly technical report. The weekly report will include, at a minimum, daily offeror activities, remedial maintenance performed and the upcoming week's activities. The monthly technical report shall include a summary of the month's activities, a status of all subsystems covered under the contract, items requiring NRC action or support and the offeror's major tasks for the upcoming month, including preventive maintenance plans. The offeror shall provide sample reports to the NRC for adjustment or approval at the award of this task or as requested by the NRC throughout the period of performance.

See sections *C.5.2.5.1 Centralized Reporting* and *Appendix E: Reporting Requirements* for a greater understanding of NRC's general reporting requirements.

C.6.3 Data Center System Administration

C.6.3.1 Project Management

The offeror's Program Manager shall meet with the NRC Project Officer to review the status of ongoing efforts and to discuss other work projects planned or proposed. Meetings will take place monthly or more frequently if desired by either party. Monthly summary reports will be provided by the 10th of each month for the preceding month. Detailed daily progress notes will be maintained for use in the monthly report, and for future reference. All work preformed off-site shall be identified in the monthly report to include at a minimum system worked on, tasks performed, and number of hours worked.

C.6.3.2 ADAMS and HLW Meta Systems

ADAMS (Agency-wide Document Access and Management System) is an electronic document and records management system that maintains the NRC's unclassified official program and administrative records in a centralized electronic document repository. The HLW (High Level Waste) Meta Systems utilizes ADAMS components as well as other Agency applications to support electronic adjudicatory hearing processes managed by the Agency. The major component of ADAMS and the HLW Meta Systems is FileNet's integrated document management software, which runs under Windows NT and Win2K, using MS SQL Server as the underlying RDBMS. The initial software FileNet suite includes Panagon Content Services, Foremost, and Panagon Web Publishing. Additional products from FileNet may be added during the life of this contract. The system also includes the custom coded Official Records Processor (ORP), and Convera RetrievalWare.

The offeror shall perform, at the minimum, all tasks required to ensure daily production support for all applications residing on current or future servers. This includes the COTS software packages and any tasks required to ensure operability as well as the application running under it. The following are the minimum support tasks required for this application. The support of ADAMS includes the production systems, test and development environments.

C.6.3.2.1 Document Storage Support

The offeror shall create new libraries/repositories and categories; maintain storage, archive and property repositories; monitor Property Manager, Storage Manager, Content Index Manager, transaction logs, index files, stop words files and other document associated files; and, develop, write and maintain quality assurance procedures for library integrity.

C.6.3.2.2 Database Support

The offeror shall perform all work necessary to maintain operability and integrity of production databases on ADAMS production servers.

In addition, the offeror shall:

1. Participate in database design processes and recommend new technologies;
2. Install all upgrades and patches;
3. Maintain ADAMS databases at the vendor supportable release level;
4. Recommend patches to the application support staff, discuss the implementation of all upgrades and patches to the ADAMS database servers and its impact on current production systems;
5. Write and/or modify scripts that will be used to maintain and monitor the production database activities. This includes scripts that monitor blocking processes, space usage, database backup and database consistency checker;
6. Monitor production disk space for both usage and fragmentation and notify application support personnel;
7. Coordinate with operating system staff in scheduling backup and restore of ADAMS database server and related file systems;
8. Write and maintain scripts and ensure that all COTS backup software correctly backup and restore all databases and associated files;

9. Notify and coordinate all restores with application support personnel;
10. Manage and support all production replication servers;
11. Perform trouble shooting of the ADAMS database server and it database issues related to hardware or software;
12. Develop and maintain procedures for the ADAMS database servers and their disaster recovery; and,
13. Maintain and perform specified disaster recovery and failover procedures.

C.6.3.2.3 Backup and Recovery

The offeror shall ensure that backup/recovery of server-installed application software, user files and datasets are done correctly; Write backup/restore scripts as needed; ensure that Mezzanine files are restored using Mezzanine procedures.

In addition, the offeror shall:

1. Write and monitor procedure/scripts to archive data from archive repositories; and,
2. Move old files to Archive Repository, delete files in Archive repository and reclaim files from archive backup (this will include interfacing with the Tivoli TSM COTS backup software and StorageTek Tape Library systems to restore files and ensure correct backup/recovery of files). Management and support of the NRC's implementation of TSM which includes multiple rotating copy pools.

C.6.3.2.4 Security Administration

The offeror shall set least privilege based default access controls for directory, library and categories; system defaults for user and group profiles; default access rights for users, groups; and set-up and manage the Administrator group, which includes adding and deleting users to the group. The offeror shall also load all OS security patches as needed.

C.6.3.2.5 Disaster Recovery

The offeror shall set up process and oversee the implementation of Long- and short-term disaster recovery. The offeror shall serve as a liaison for the NRC with a third party offsite DR vendor and document and test recovery procedures, as well as ensure that the third party vendor is aware of any changes to the configuration or procedures.

C.6.3.2.6 Performance and System Monitoring

The offeror shall monitor and analyze system parameters and interpret performance reports to identify bottlenecks, predicate response time and throughput changes. The offeror shall check for aborted sessions and delete sessions.

In addition, the offeror shall:

1. Re-map storage managers;
2. Monitor system utilization, space management, disk usage;
3. Monitor the number of users added and the impact on system performance;

4. Check disk space and redirect libraries when need for disk performance; Redistribute categories to other repositories when needed;
5. Monitor System messages sent to Administrator group message area;
6. Maintain the custom properties and set up new ones as directed;
7. Monitor Stopword files; and,
8. Provide recommendation to application developers and users to enhance application performance.

C.6.3.2.7 Systems Administration

The offeror shall install software such as Mezzanine, FileShare, and Foremost including new releases and patches as well as any new products associated with ADAMS that reside on the Server. The offeror will also Install and provide production control of all new releases of the application software residing on the Server. This includes changes to the files structure, and default setting of Mezzanine.

In addition, the offeror shall:

1. Diagnose and resolve problems related to the server, network, Mezzanine/ FileShare, Microsoft SQL server, including interface with client, application developer, and NT systems administrator to resolve bugs and error messages;
2. Integrate and test ADAMS related software with other packages on the server;
3. Write and implement server scripts if needed for such things as backup, AT jobs, product outputs or any other function as related to the Mezzanine software including Microsoft SQL Server;
4. Define printers needed for output as related to server and the Mezzanine software;
5. Insure the production test environment is compatible with production;
6. Release changes to production as approved by the ADAMS administrator;
7. Interface with the helpdesk, network operation center, support groups, et al; coordinate applicable activities with hardware and software maintenance contract personnel;
8. Make recommendations for new hardware, software, or procedures that increase performance or availability;
9. Ensure that the operating system and FileNet server software in production is at a supportable release;
10. Assist with testing of new releases of operation systems software with the application and operating systems personnel to insure that FileNet software is compatible;
11. Allocate disk space and reformat disk space as need to ensure optimum performance of the application;
12. Provide operator training and/or documentation for any production scripts, and establish/maintain a CD/ROM library of installed software;

13. Maintain and document installation information, trouble shooting techniques, problems encountered, configuration information and default settings; and,
14. Set up and maintain clustered servers.

C.6.3.3 Mainframe Administration

The NRC utilizes the Department of the Interior National Business Center for payroll services and the National Institutes of Health (NIH) mainframe for a variety of support systems. Offeror personnel shall perform, at the minimum, the following tasks in order to ensure optimum system support and availability of the Department of Interior (DOI) and National Institutes of Health (NIH) IBM mainframe systems:

C.6.3.3.1 Application Support

The offeror shall respond to user inquiries on technical matters such as: resolving programming anomalies, access to and use of equipment, systems software, and support for vendor or third-party proprietary software. The offeror shall work with the telecommunications staff to facilitate communication setup and problem resolutions.

In addition, the offeror shall:

1. Rectify problems with communication setup as appropriate;
2. Allocate disk space for system file, users, and databases and their associated tables;
3. Interface with the NIH on behalf of the NRC as requested. These duties are performed in accordance with the guidelines set forth by NRC;
4. Run the monthly timesharing cost reports and monitor account usage and resource usage;
5. Support Agency remote job entry (RJE) and IP print services, write and maintain scripts to assist with print distribution and redirection;
6. Support file transfer to other agencies using various transfer protocols, such as Systems Network Architecture (SNA), and TCP/IP;
7. Troubleshoot problems to determine if they are communications, hardware, application, or system related. Discuss findings with NRC Project Officer and recommend corrective action;
8. Implement resolution and/or facilitate activities of telecommunications personnel or hardware/software vendor engineers, as appropriate;
9. Perform impact analyses of proprietary and systems software upgrades to existing applications as well as on new software and hardware;
10. Develop and maintain data dictionaries as required;
11. Support, revise, and develop standards for database structures, table and field names, table relationships, and security protection schemes; and,
12. Advise application developers on matters of database efficiency and integration.

C.6.3.3.2 Systems Administration

The offeror shall perform system administration duties to include disk pack formatting, system generation, and device configuration as necessary. The offeror is also responsible for allocating disk space for system file, users, and databases and their associated tables. At award of this task, and when the NRC believes that changes are appropriate, the offeror shall make recommendations on standards and procedures for performing system administration and device configuration. The NRC will review, make recommendations for adjustment and approve these recommendations for use. The offeror shall then use these standards throughout the period of performance.

In addition, the offeror shall:

1. Develop and maintain systems software, computer and telecommunications hardware documentation, as required;
2. Load and test system software and system software upgrades as necessary;
3. Maintain operator proficiencies in the use of software, procedures and macros;
4. Facilitate the hardware maintenance vendor's diagnosis and repair of equipment by running specific operating system software until repairs are completed;
5. Support, revise, and implement system safeguards such as directory structures, access controls, and procedures;
6. Maintain user profiles, support, revise, and implement standards for assignment of privileges;
7. Develop a schedule to install and test proprietary and executive system software and utilities that will ensure that all software revisions fall within vendor support windows, provide the latest/most needed functionality, and at the most current patch levels;
8. Coordinate installation with programmers and end users after obtaining approval from the NRC Project Officer;
9. Provide systems support to contract and in-house users of vendor or third party related proprietary software;
10. Monitor system performance and identify system changes/modifications needed to assure systems are running efficiently and effectively. This is to include monitoring disk usage and performance. Discuss findings with NRC Project Officer, recommend corrective action, and implement resolution; and,
11. Develop hardware and software test plan and upon approval by the NRC, perform hardware and software integration and testing.

C.6.3.3.3 Backup and Recovery

The offeror shall design and implement system backup and restore procedures to ensure that the NRC systems are maintained with complete backup and have the ability to be restored.

In addition, the offeror shall:

1. Perform a daily backup of NRC's private Direct Access Storage Devices (DASD), and/or as specified in NRC Backup and Recovery System documentation for the backup system;
2. Enhance and/or modify the backup and recovery programs as needed (with prior approval of NRC Project Officer);
3. Maintain the inventory of backup data used by NRC at the NIH timeshare facility; and,
4. Maintain up to date backup data inventory, per the NRC Backup and Recovery System documentation.

C.6.3.3.4 Training

The offeror shall provide training to on-site personnel on the uses of new software, procedures, and macros as implemented. The offeror shall be responsible for providing system support to NRC Computer Operations staff as needed to facilitate the successful operation of NRC computer systems. The offeror shall provide any needed assistance to NRC or other contractors in the transition of any of the listed applications to a new computer environment.

C.6.3.4 HRMS

The HRMS systems currently consists of PeopleSoft, Human Resources (HR) and Time & Labor and Benefits modules which interfaces with the HR/Payroll system running at DOI. The current implementation runs on 3 Sun Enterprise 5500 servers using PeopleSoft 7.5, Sybase ASE V12, Sybase Replication Server and Tivoli Workload Scheduler. The system is currently undergoing an upgrade. The scope of effort includes the production, failover and pre-production environments. Server Administration task information will be provided when the new system is implemented.

C.6.3.4.1 PeopleSoft Application support

The offeror shall monitor the performance and availability of the application server and process scheduler; review output files; perform migrations and debugging migration problems. Run SysAudit reports; apply custom code updates and fixes as required; and, document all PeopleSoft production procedures for the systems and data center teams.

C.6.3.4.2 Database Support

The offeror shall perform all work necessary to maintain operability and integrity of production databases on HRMS production servers.

In addition, the offeror shall:

1. Participate in database design processes and recommend new technologies;
2. Install all upgrades and patches;
3. Maintain HRMS databases at the vendor supportable release level;

4. Recommend patches to the application support staff, discuss the implementation of all upgrades and patches to the HRMS database servers and its impact on current production systems;
5. Write and/or modify scripts that will be used to maintain and monitor the production database activities. This includes scripts that monitor blocking processes, space usage, database backup and database consistency checker;
6. Monitor production disk space for both usage and fragmentation and notify application support personnel;
7. Coordinate with operating system staff in scheduling backup and restore of HRMS database server and related file systems;
8. Write and maintain scripts and ensure that all COTS backup software correctly backup and restore all databases and associated files;
9. Notify and coordinate all restores with application support personnel;
10. Manager and support all production replication servers;
11. Perform trouble shooting of the HRMS database server and it database issues related to hardware or software;
12. Develop and maintain procedures for the HRMS database servers and their disaster recovery; and,
13. Maintain and perform specified disaster recovery and failover procedures.

C.6.3.4.3 Disaster Recovery

The offeror shall provide support for failing over the production environment to the warm standby environment located in a specific NRC facility or a primary disaster recovery site as designated by the NRC. The offeror is also responsible for updating the failover documentation as necessary to reflect current operational configurations.

C.6.3.4.4 Performance System Monitoring

The offeror shall work in concert with the UNIX support team to isolate client, server and database issues in a timely manner. The offeror also reviews system logs, emails and performance data daily to ensure optimum system operation.

C.6.3.4.5 System Administration

The offeror shall install OS upgrades and security patches including new releases of Tivoli Workload Scheduler. The offeror provides training to other systems staff and data center operators as needed.

In addition, the offeror shall:

1. Create an automated mechanism (e.g. UNIX shell scripts) to monitor system and application health that alerts systems and data center staff in the event of an error condition;
2. Perform periodic refreshes of the Pre-Production environment as requested;

3. Synchronize client files on remote servers and the failover system. Interface with the helpdesk, network operation center to resolve problems;
4. Coordinate applicable activities with hardware and software maintenance contract personnel;
5. Make recommendations for new hardware, software, or procedures that increase performance or availability; and,
6. Maintain backup jobs and schedules. Add new jobs, or modify existing jobs as needed

C.6.3.5 Production Database Management

The offeror's personnel shall perform all work necessary to maintain the operability and integrity of production databases on all production servers. The following tasks are associated with this function. This administration will be required for current and future NRC production databases.

C.6.3.5.1 Application patching

The offeror shall install upgrades and patches to the production environment. All databases will be maintained at a vendor supportable release level. Patching must be maintained to the service levels outlined in *Appendix A: SM-SLA-009: Service Design Lifecycle Support.*

In addition, the offeror shall:

1. Recommend patches to the application support staff, discuss the implementation of all upgrades and patches to RDBMS servers and its impact on current production systems; and,
2. Assist in the check out process to insure that new releases do not impact the overall production system or operating system.

C.6.3.5.2 Production Scripts

The offeror shall write or modify scripts that will be used to maintain, and monitor the production activities. This includes scripts that monitor blocking processes, space usage, database backup and database consistency checker.

In addition, the offeror shall:

1. Place into production and maintain any application specific scripts developed by the applications support staff that are required to maintain the production application;
2. Automate error reporting to notify systems and data center staff;
3. Provide training for the data center operators to respond to the error messages by facilitating escalation during off hours; and;
4. Maintain any scripts that are run on a regular basis that modify the data.

C.6.3.5.3 Disk Space allocation

The offeror shall monitor the production disk space for both usage and fragmentation and notify the application support personnel when either more space needs to be allocated or when the existing space has become fragmented then increase or reallocate the space as agreed upon with support personnel.

C.6.3.5.4 Database Design

The offeror shall provide comments and information about the current productions system and infrastructure to ensure that the new database integrates correctly into the current environment. The offeror shall also provide guidance and support to application developers to improve application performance, debug application problems and provide guidance on database security.

In addition, the offeror shall:

1. Make recommendations for new server and hardware to existing servers that will increase performance and uptime;
2. Recommend new solutions and hardware as it becomes available; and,
3. Evaluate solutions with respect to the production environment and the infrastructure.

C.6.3.5.5 Backup and Recovery

The offeror shall coordinate with Operating System staff in scheduling backup/restore of RDBMS server related file systems. The offeror shall also write and/or maintain scripts or insure that all COTS backup software correctly backup and restores all databases and associated files.

In addition, the offeror shall:

1. Notify and coordinate all restores with application support personnel;
2. Manage Replication Server; and,
3. Maintain and support all production replication servers.

C.6.3.5.6 Troubleshooting

The offeror shall perform trouble shooting of the RDBMS Servers and its database issues related to hardware/software. Problems on the production systems shall have trouble shooting conducted with the assistance of Application support personnel when needed. All problem resolutions will be discussed with support personnel to determine that the fix will have minimally adverse impact on the application. The offeror shall also inform application support personnel, the Production Environment Manager, and the Help Desk if any problems occur and consult with them about the resolution of such problems.

C.6.3.5.7 Documentation

The offeror shall develop and maintain procedures for the RDBMS servers and their database disaster recovery. The offeror shall also maintain and perform specified disaster recovery and failover procedures as well as maintain and document production installation

information, trouble shooting techniques, problems encountered, configuration information, and default settings.

C.6.3.6 NRC Web Servers and Three Tier Environments

The NRC Internal and External Web Sites reside on Sun Unix platforms. Each web environment consists of a reverse proxy, a web server that also runs an application server, two database servers and an authentication server. The external web platform also includes Cisco load balancers. There are production, test and development environments. The software currently consists of Solaris OS, Win2k, Sun iPlanet, ColdFusion MN, Sybase, and MS-SQL Server. The following are the minimum support tasks required for this application. The support of NRC Web services currently includes the production systems, and development environments.

C.6.3.6.1 Web Server Support for iPlanet and Coldfusion

The offeror shall provide support for both external and internal Web servers by monitoring the performance, reviewing system logs, and applying security and functional patches.

In addition, the offeror shall:

1. Provide performance tuning and trouble shoot problems;
2. Manage the migration of application changes, patches and configuration changes to production from the test environment;
3. Load software to the development environment and monitor the server;
4. Assist developers and testers during development phase; and,
5. Run and set up Web usage reports.

C.6.3.6.2 Performance and System Monitoring

The offeror shall monitor and analyze system parameters and interpret performance reports to identify bottlenecks, predicate response time and throughput changes. The offeror shall also provide performance tuning, make recommendations for improvements, including additional hardware or software that increase performance and maintain system capacity as well as respond to messages from the web monitoring service.

C.6.3.6.3 Backup and Recovery

The offeror shall ensure system backup and recovery meets needs of business owner. The offeror shall also coordinate with and assist with Disaster Recovery planning and provide assistance as needed for the disaster recovery plan.

C.6.3.6.4 System Administration

The offeror shall install upgrades and security patches for OS and other system software residing on the server. The offeror shall also write and maintain system maintenance jobs using shell scripts and PERL.

In addition, the offeror shall:

1. Coordinate hardware maintenance with vendor;
2. Configure and maintain Cisco content switches;

3. Interface with Help Desk network operations center to resolve problems;
4. Coordinate with Consolidated Test Facility (CTF) as needed to move system into production; and,
5. Coordinate applicable activities with hardware and software maintenance contract personnel.

C.6.4 Wireless Communications Services

This section describes the specific requirements, using the NRC ITISS contract vehicle, for managing and maintaining the Agency's wireless communications management in support of the Agency's mission.

C.6.4.1 Telecommunications Management and Oversight

The offeror shall provide telecommunications services in the form of technical advice and assistance to the Government to ensure that telecommunications services that are ordered meet the Government requirements and provide recommendations to the Government to ensure that services that are no longer needed are removed.

Currently, the NRC BlackBerry infrastructure is divided among two separate contracts. One contract supports the BlackBerry Enterprise Server (BES) environment, provisions BES accounts, and manages the device policy settings. The other contract supplies devices, service plans, help desk services, and maintenance of devices. This optional task encompasses the device provisioning, service plans, help desk and maintenance piece. The intent of the NRC is that, once this task is awarded, the services under this task will be blended with existing tasks under the core services such as *C.5.1.1 BlackBerry*, *C.5.2.3.3 Service Asset and Configuration Management*, *C.5.2.2.7 Supplier Management*, *C.5.2.4 Service Operation*, etc.

In addition, the offeror shall:

1. Provide telecommunications billing analyses to ensure that the billing accurately reflects what the offeror ordered on behalf of the Government and that there are no erroneous charges;
2. Analyze and make recommendations to the Government on changes that should be made to billing plans and devices with the overall goal to reducing additional costs to the Government based upon usage information;
3. Brief the NRC Project Officer on IT/Telecommunications operating procedures on an as needed basis and make recommendations to the Government on how to improve customer services issues and internal processes;
4. Maintain accurate copies of the offeror's service agreements, contracts, and other records with wireless carriers that specify the pricing, terms and conditions of wireless services providers that are procured under this contract;
5. Monitor offeror spending levels, service line counts, or other measurable indicators that have been agreed upon between the Government, the offeror and the carriers;
6. Meet on a quarterly basis with the Government to develop strategies and obtain guidance for dealing with carrier contract related issues, practical strategies for

achieving optimal pricing or service terms, and methods to maximize negotiation strength with carriers;

7. Advise the Government on how their contracts or agreements might be impacted by changes in the wireless telecommunications industry or by new wireless service offerings and assist with developing strategies to include new, or terminate old, technical services into their carrier contracts or agreements;
8. Perform database reconciliation and maintenance for the ICOD Computer Operations and Telecommunications Branch (COTB) NRC Space and Property Management System (SPMS) inventory holdings and Work order Processing and Tracking System;
9. Update and maintain the Work order Processing and Tracking System in response to work orders for those work orders for which the offeror is responsible for fulfilling; and,
10. Develop documentation or Standard Operating Procedures (SOPs) that define the offeror's use of the SPMS, Work order Processing and Tracking System and the Telecommunications Expense Management tool and their use in the course of providing services under the contract.

C.6.4.2 Project Status Reports

C.6.4.2.1 Monthly Status Reports

The offeror shall provide a Monthly Status Report which shall cover activity of the previous month and be delivered on the tenth workday of the current month. The report shall include, but not be limited to:

1. The number of requests for property and property control forms processed as defined in the current SOPs;
2. The number of requests for repair/maintenance of trouble calls processed and their current disposition as defined in the Telecommunications Service Center (TSC) SOPs;
3. Equipment totals by carrier, manufacturer, and model which lists the number received, number distributed, number excessed, number un-reconciled (location/user unknown),and the number on hand (at the TSC, warehouse, and other designated NRC locations), recommendations for any additional purchases;
4. An updated list of deliverables with completed or scheduled delivery dates;
5. Identification of un-reconciled equipment items where "un-reconciled equipment" is defined as any equipment the TSC is unable to locate the device or determine that there was a properly signed NRC Form 119 (receipt for property) in the TSC for a tagged and/or sensitive item;
6. Any problems, conflicts, staffing or other concerns and recommendations for resolution;
7. Contract expenditures Fiscal Year to Date and Contract to Date for both labor and other direct costs along with an end of fiscal year projection based upon known projects and current burn rate;

8. Prepare monthly reports identifying billing and invoicing errors;
9. Prepare monthly standardized management reports detailing spending levels and trends. Generate custom-designed and ad hoc spending reports at both a summary and various organizational or financial account levels;
10. Deliver standard reports as specified by the Government in the contract. Delivery of reports shall be facilitated by a web-based "download and save" capability through a reporting portal or through direct delivery to the Project Officer and Contracting Officer;
11. Provide standard reports on each of the reporting areas that details and organizes the information by the Government's designated organizational breakdown or reporting structure and wireless telecommunications service provider; and,
12. Provide standard management reports identifying the payment status of invoices, balance of any obligated Government funds under the contract and any received invoices awaiting payment or affected by a dispute or claim.

C.6.4.2.2 Weekly Status Reports

The offeror shall provide a Weekly Status Report due by close of business of the second business day of each week that shall include, but not be limited to the following information as required by the Government:

1. The number of services requests received via the NRC service desk service request system. The Service desk is manned by another contractor and generates both work orders and service request to which the offeror responds for
    - Federal Calling Cards;
    - Government Emergency Telecommunications Services cards;
    - Cellular telephones;
    - Wireless Priority Service;
    - BlackBerry;
    - International cellular phones or BlackBerry;
    - Porting of cellular telephone numbers; and,
    - Wireless cards.
2. The number of current International cellular telephone and BlackBerry devices on loan;
3. The number of pending/outstanding service requests over one week old; and,
4. Identification of any reported lost or stolen devices from the Office of Information Services/Telecommunications (OISTEL) property account as defined in the NRC SPMS inventory listing.

C.6.4.3 Telecommunications Support Services

Telecommunications support services are those services that are needed to support the Government's requirements for property management, service and equipment ordering, rate plan optimization, billing, billing verification, dispute resolution, support for billing analysis and telecommunications services recommendations as requested.

C.6.4.3.1 Maintenance of Property Management Records

The offeror shall update, on a daily basis, the telecommunications expense management (TEM) tool and reconcile the TEM with the NRC SPMS database (i.e. the NRC official property database). The offeror shall add additional fields to aid in property accountability as necessary to the TEM tool functionality to meet the Government requirements.

C.6.4.3.2 Wireless Hardware and services

The offeror shall perform the following types of general support in accordance with SOPs.

1. Inventory and reconciliation of the wireless inventory of services and hardware in the Office of Information Services (OIS) Infrastructure and Computer Operations Division (ICOD) Computer Operations and Telecommunications Branch (COTB) NRC Space and Property Management System (SPMS) property account and the telecommunications expense management (TEM) tool;
2. Property storage and control of on-hand wireless hardware;
3. Service request processing using both the Government provided service desk ticket request system and the TEM tool to process and fill the appropriate orders to meet the Government's approved requirements;
4. Property distribution/return;
5. BlackBerry server support in the area of assisting the Government in identifying service problems for the end users that may make their appearance known on the server; such as a missing PIN, etc;
6. User device/service training to ensure that the user is familiar with the device they are issued; to allow them to place and receive cellular calls; unlock their BlackBerry, the procedures for charging and caring for the devices, etc;
7. Coordinating with the wireless carriers and the Government customer on the movement of a cellular number from one device to another using the same carrier or between carriers;
8. Pairing Bluetooth hardware (headsets, vehicle mount, vehicle charger, and GPS navigation utility, etc.) with cellular devices when requested; and
9. Preparing cellular phones and BlackBerry devices for issuance in the fulfillment of an authorized work order.

Currently, the NRC is satisfied with BlackBerry devices and the interconnections with the agency's email system. The NRC is open to other mobile computing devices over time (See *C.5.1.4 Personal Computing and Related Software Licensing*). However, the NRC would like to maintain a standard with a manageable set of devices and does not want to incur significant costs or complexity associated with managing too many mobile platforms.

C.6.4.3.3 Products and Services

The offeror shall coordinate with various telecommunication carriers to provide to the NRC, wireless communication products and services that will cover equipment, service plans, delivery times, carrier related warranty information for new equipment and maintenance. Following Government approval for a wireless product and service, the offeror shall order

the approved wireless product/service with a normal delivery time of 3 to 5 business days. If the wireless product or service is required immediately, the order shall be expedited. All hardware becomes the property of the Government while the wireless plans will belong to the offeror.

C.6.4.4 Telecommunications Expense Management Services

The offeror shall propose a Telecommunications Expense Management (TEM) software solution that may be leased or owned by the offeror as an optional service to the Government. If elected, the following shall be true:

The offeror shall maintain, on behalf of the Government, the cellular accounts and service relationships with the carriers related to wireless services. The user community for the TEM tool will be those offeror employees who, under this contract, require access to perform their duties; as well as authorized Government personnel who need to monitor their tasks as performed under this contract. The offeror shall utilize TEM software which shall allow the offeror to take necessary action to maintain an accurate master inventory of all wireless devices and services in current use by the Government. Inventory accountability shall be maintained from requisition through disposal or final disposition of the service line and device.

In addition, the offeror shall:

1. Maintain and perform the moves, adds, changes, and deletions (MACDs) of service lines and devices in order to maintain the accurate master inventory of services and devices;
2. Generate and deliver to the Government inventory managers both standard periodic inventory reports as well as custom-designed and ad hoc reports at both a summary level and at various organizational or inventory account levels, depending on the level of detail and information provided by the Government;
3. Collect, process, and validate paper and electronic invoices received from multiple carriers in multiple billing formats against Government information, ordering records, and wireless and land line contract or service agreement terms maintained in the offeror's data system;
4. Audit all carrier invoices billed to the Government on a monthly basis in an effort to realize audit savings on behalf of the Government;
5. Allocate cost information from the carrier invoices across the Government's organizational units or financial accounts to provide increased visibility and accuracy for the Government's cost and spend management functions;
6. Integrate invoice data with offeror's procurement and inventory management data records to enable and support the spend, inventory and usage analysis by the offeror and authorized ICOD/COTB/ Telecommunications Team (TT) personnel;
7. Support periodic Government audits of inventory accounts by providing inventory listings and cooperating with Government audit officials as they perform their duties;
8. Provide recommendations for rationalization of rate plan types, number of service lines with specific carriers, the number of total carriers, and other opportunities that might lower total cost while maintaining or improving the quality of wireless service

provided to the Government's users. Account and rate plan changes should be made to lower future costs;

9. Continually track and report savings derived from the rate plan optimization efforts on at least a quarterly basis;
10. Perform a comprehensive assessment of the Government's existing wireless and land line contracts and agreements to identify improvement and cost savings opportunities;
11. Make specific recommendations for rationalization of rate plan types, migration of service lines between specific carriers, changing the number of total carriers, changes in cellular plan contract terms & conditions, and other opportunities that might lower total cost while maintaining or improving the quality of wireless and land line service provided to the Government's users;
12. Work with the Government to carry out and implement approved contract optimization recommendations, changes, and sourcing/competitive bidding among carriers intended to lower overall total cost. Track and report savings derived from TEM contract optimization efforts;
13. Provide a centralized web-based ordering portal to facilitate the requisition of new wireless and land line services (future), devices, and accessories from Government-approved suppliers;
14. Provide automation of procurement transactions across multiple wireless carriers including MACDs and their necessary Government coordination and approvals;
15. Integrate and align ordering and procurement processes with Government personnel and manpower systems taking into consideration multiple approval hierarchies and functional or business units;
16. Track orders and change orders from order initiation through delivery and entry of the asset's information into the Government approved property management system;
17. Provide Government-specific help desk support Monday-Friday between the hours of 7:00 a.m. to 5:00 p.m. (EST) to assist Government customers and telecommunications managers with procurement and ordering support;
18. Provide ongoing services to receive, validate, code for chargeback, and, pay (upon receipt of Government funding designated for payment) all wireless telecommunications service provider invoices;
19. Provide on-going support services as necessary to update and maintain the accuracy and currency of account lists, supplier, and Government information in the TEM provider's data and payment systems as directed by the Government;
20. Assist the Government by identifying opportunities and facilitating account consolidation efforts with individual wireless providers to streamline payment processes;
21. Collect and prepare support material necessary to file and defend claims submitted to the carriers for billing and account corrections;

22. Research, review, dispute, and track all potential billing errors and represent the Government as an authorized agent with all carriers and wireless telecommunications suppliers; and,
23. Submit written claims to carriers (both landline and wireless) and suppliers, including reasonable and necessary support documentation, to identify and recover any claimed amount for the Government. Handle and track all claims through final resolution.

C.6.5 Software License Management

This section describes the specific requirements, using the NRC ITISS contract vehicle, for a comprehensive inventory of Agency software licenses, the negotiation and management of those licenses, and the Agency-wide procurement and distribution of software.

C.6.5.1 Software Inventory

The offeror shall conduct a series of interviews and reviews to develop a comprehensive inventory of all software licenses owned by the NRC for both commercial-off-the-shelf software (COTS) as well as custom developed software.

The offeror shall use automated discovery tools to determine what software is installed on the NRC ITI to assist in the inventory interview process, and to confirm what is discovered in those interviews. The offeror shall ensure that multiple methods are used to determine what software is actually installed on every computer (i.e. Add/Remove Programs, MSI Database, EXE/DLL Header information, Windows Registry, etc.). The offeror shall reconcile the electronic inventory with the physical inventory and identify any discrepancies.

The offeror shall include any offeror-controlled software assets in this software inventory exercise.

The offeror shall provide a detailed report of the inventory to include software licenses owned by the Agency that are not installed on Agency computer systems (over-licensing), software installed on Agency computers that are not properly licensed (under-licensing), and physical locations and holders of all software licenses.

C.6.5.2 Planning and Design

The offeror shall make recommendations on how the NRC should centrally manage its software assets. These recommendations shall include the steps necessary to move from the current state of software management to the desired state of central control.

The offeror shall make recommendations for how the NRC should negotiate enterprise license agreements with COTS software vendors. The offeror shall make recommendations related to best practices for software as a service, software ordering, virtual desktop access, and other approaches to maximize user access to software tools and manage software costs effectively.

The offeror shall recommend multiple alternatives, with a preferred approach, for how the software inventory will be kept up-to-date. This approach will take into consideration the various software needs of NRC IT users and existing process workflows.

With NRC approval, the offeror shall implement, maintain, manage, patch, and upgrade the recommended Software Licensing management approach.

C.6.5.3 Software License Management Tool

The offeror shall recommend the appropriate tool or tools to manage Agency software license and asset information. This tool shall integrate with the offeror's configuration management database that is used under the ITISS contract. At a minimum, this software will track software licenses, computers that software is installed upon, users with access to software, vendor information, software version and upgrade information, and physical location of license (if any).

With NRC approval, the offeror shall implement, maintain, manage, patch, and upgrade the recommended Software License Management tool.

C.6.5.4 Enterprise License Vendor Management

The offeror will assist the NRC in negotiating with software vendors on obtaining enterprise licenses for Agency software. In those circumstances where it is inappropriate to seek an enterprise license, or the vendor does not offer an enterprise license, the offeror shall work with vendors and the NRC to obtain the most suitable license arrangement possible (i.e. Concurrent User, Per Server, Client/Server Access [CAL], Volume, etc.).

The offeror shall also track and assist the NRC with the management of Vendor agreements for software licenses.

C.6.5.5 Software Catalog

The offeror shall provide, manage, maintain, and keep updated a comprehensive list of software that can be purchased by NRC users through the ITISS contract. The offeror shall integrate this Software Catalog into the IT service Catalog that is maintained by the offeror.

The offeror will provide, as a part of the Software Catalog, an automated mechanism for users to order software for their use. Users will be able to track the progress of their order through submission, to approval, and through installation.

The offeror will work with Agency program and support offices and will integrate their approval workflows into the software ordering process. The offeror will interface with Agency financial management tools to track the funding available for software purchases and the purchase of software licenses.

Once a user's request has been approved, and funds have been made available, the offeror shall procure the appropriate software license and make the software available to the user (including distribution to remote users). The offeror shall notify the user of software availability, and will follow-up with the user to make sure that the user can access the software and that their request was met.

The offeror shall record the license purchase in the Software License Management Tool and track the license through its lifecycle.

C.6.5.6 Usage Reporting and Auditing

The offeror shall be able, at any time, to produce reports related to software licenses at the NRC. The reports shall link specific licenses to where those licenses are being used and by whom.

The offeror shall report any license breeches, whenever they occur to the NRC Project Manager.

On a monthly basis, the offeror shall provide a report of software in use, including the number of installed copies of that software, the total number of software licenses allocated, and the number of software licenses actually being used. The offeror will provide a separate monthly report of any unused software licenses, by product, itemizing the total number of licenses available. This shall include tracking multiple users and/or concurrent usage data, including usage for applications hosted in a Citrix environment.

The offeror shall make quarterly recommendations as to changes in the Agency's licensing approach. The offeror shall track changes in licensing practices by vendors and look at trends in Agency user software purchases. As the Agency's software portfolio matures, there may be opportunities to save on software costs or modify the way in which software is delivered. The offeror shall evaluate these changes and make recommendations for best practices for software management on an on-going basis.

The offeror shall perform an annual physical audit of software licenses in the Agency. This physical audit will be compared to both an electronic audit as well as the Software License Management Tool maintained as a part of the configuration management database. A complete report of any discrepancies between the physical audit, electronic audit, and CMDB will be provided by the offeror.

The offeror shall make recommendations for the retirement of software assets based on trends in the annual audits and monthly usage reports. The offeror shall be guided by Agency Technical Reference Model recommendations for software retirement, and support the Agency's effort to remove these recommended software products from the environment.

See sections *C.5.2.5.1 Centralized Reporting* and *Appendix E: Reporting Requirements* for a greater understanding of NRC's general reporting requirements.

The offeror shall be responsible for ensuring that the software on all computing devices (desktops, laptops, servers, BlackBerrys etc.) is fully licensed. The offeror shall be financially responsible for any license non-compliance for offeror-managed software packages. Audits of software licensing will be performed on all devices by an independent verification and validation contractor. The offeror shall bring licenses into compliance for any discrepancies identified in those audits for offeror-supplied software packages.

C.6.6 Safeguards Local Area Network and Electronic Safe Services

This section describes the specific requirements, using the NRC ITISS contract vehicle, for providing O&M services for the Safeguards LAN and Electronic Safe (SLES) system.

It should be noted that secure wireless access described herein is specific to the SGI LAN and is distinct from wireless access within the NRC or remote access to the NRC for Personal Computers.

C.6.6.1 General

The SLES consists of two distinct components, SGI LAN which operates as a General Support System (GSS) and E-Safe as a Major Application on the SGI LAN. The SLES provides a secure communications platform for the authorized users to access, create, and collaborate on SGI. Technically, the system consists of backend equipment located in secure server rooms connected via encrypted wireless or wired links to thin client devices at the users' desks. KVM switches are used to isolate the SLES network from the NRC network at the user's workstation along with strong user authentication controls through Smart Card, NRC Managed Private Key Infrastructure (MPKI), and hardened network operating systems. Network connection to users in the Regional offices and NRC Inspector

Offices at the power plants is through NRC's LAN/WAN routers using system-specific TCP/IP VLANs and users outside of the NRC network through VPN.

This task consists of, but not limited to, system and security administrative activities, tasks and activities for maintaining the SLES equipment Hardware (HW) and Software (SW) with the exception of the E-Safe Record Management software administration and SGI documents and records residing within E-Safe repository. The SLES equipment HW and SW includes the SLES equipment deployed at the user's desk (Thin client terminal, KVM switch, etc.) as well as the infrastructure equipment (Wireless Access Points, controllers, switches and routers, etc.). The offeror shall be also responsible for providing Help Desk and operational user support services for SLES. The offeror shall ensure that both key and backup personnel are committed in providing operations and maintenance support services during service hours as indicated under *C.5.1.5 Network Components*. All service requests (telephone call, email, or other means of communication) must be responded to by the offeror within a 60 minute time-frame from the time that the service request was received.

In case of emergencies or for reasons related to system repair/maintenance, the offeror may be called or required to work at any time.

In addition, the offeror shall:

1. Maximize the availability of the SGI Wireless Network (i.e. minimize the length and frequency of service outages);
2. Minimize the discrepancy between date of a given scheduled system backup and date on which that system backup occurs; and,
3. Minimize the time from when an unusual file storage growth pattern is identified to when the appropriate staff members are notified.

C.6.6.2 System Administration

Monitoring the performance of all SLES back-end servers and other equipment, systems programming and configuration management, database administration, security hardening, building of new servers, hardware/software configuration, system backup and restore, system review and making recommendations for performance enhancement are included under this task.

C.6.6.2.1 Performance Monitoring

The offeror shall continuously monitor the performance of all SLES system hardware and software with the exception of the Record Management software, to identify and resolve problems that may arise on a daily basis. This includes monitoring and testing of new or additional servers and equipment that may be added as part of the network system. The offeror shall be responsible for monitoring and testing of the Wireless Access Points (WAPS) for bleed outside of the facilities approved for wireless SGI processing. Bleed shall not be more than 10-15 feet outside the approved buildings. The system administrator shall review all application specific logs associated with the servers (i.e. server logs, database logs). The offeror shall notify the NRC project officer of any problems identified and obtain approval from the NRC project officer before taking actions for resolving them. All incidents, issues or concerns must be recorded by the offeror in the "Maintenance and Activity Log".

The system administrator shall monitor Central Processing Unit, memory and disk performance of all system servers as it expands from the current stage of development to deployment at the regional offices and other authorized Federal, State and Local Government Agencies and Licensees.

The administrator shall look for any unusual activity that may represent potential threats or issues with system performance.

The offeror is responsible for maintaining a proactive security stance by accurately documenting routine and non-routine actions occurring on all SLES servers. The Maintenance and Activity Log shall be kept updated for all SLES system servers. All issues identified as a result of these activities will be escalated following the procedures outlined in the system Operations Manual.

The system administrator shall also document all system abnormality occurrences that cannot be accounted for in the audit logs. The information recorded will include the name of the server, the name of the administrator, the date of the occurrence, the details of the abnormality, any actions taken to remedy the situation, whether or not further action is required.

C.6.6.2.2 Backup

This task consists of producing daily (Monday – Friday) incremental tape backup of all the SLES servers and a full backup once a week. System backups must be retained for a period of at least one month on tapes or data mirror server.

The offeror shall be responsible for managing the rotation (shipping and receiving) of the backup tapes to a geographically remote location from the NRC Headquarters for storage.

C.6.6.2.3 Recovery

This task ensures that the data is recoverable from the backup tapes.

The offeror's designated system administrators (may be referred to as the system administrator, administrator or offeror hereafter) shall perform verification tests to restore several different files from the tapes to temporary directories on various servers. The verification test may be performed on the SLES test and development environment when available. Temporary files will be deleted after verification is complete.

Verification tests of the backup system must be performed at least once every quarter and shall be documented in the Maintenance and Activities log. Procedures for data recovery "verification" test shall be developed and presented by the offeror to the SLES project manager and the Information System Security Officer (ISSO) for approval.

C.6.6.2.4 Image Backup

The offeror shall maintain a standard user and kiosk terminal images on backup tapes once a week in order to capture and maintain standard configuration of the terminals.

The system administrator shall identify the standard user and kiosk terminal that the images will be made from. Using the Rapport utility, the system administrator shall create (read) an image of the target user desktop terminal for storage and distribution. Device identification numbers along with the users ID and all other device deployment related data are maintained by the SLES the system administrator in the Rapport server.

C.6.6.2.5 Database Administration

The offeror shall provide database (SQL server) administration functions on the SLES system. This task includes database structural maintenance activities, adding tables and repositories as needed as well as first line database related support to users, troubleshooting user issues, administering user privileges and assistance to users in generating reports. NRC project manager and ISSO approval must be obtained before changes are made to the database.

C.6.6.3 User Support

C.6.6.3.1 Access

The offeror's designated security administrator shall administer user registration (addition and removal of users) based on established procedures outlined in the SLES Operations Manual. The offeror must also maintain an active SLES user list. This activity includes set up and removal of the SLES user desktop equipment. In conformance with NIST standards, SP 800-53, separation of duties through system access authorization must be assured between the system administrator and the system security administrator who is in charge of access card issuances/cancellations and the system access control administration.

C.6.6.3.2 Helpdesk Support

The offeror shall provide help desk services through an NRC established phone number and email. Dedicated on-site staff shall be available during the core hours of 7:00 am through 5:00 pm EST. In addition, the offeror shall be on-call and may be asked to support users at any time after the business hours (24 hours/day 7 days per week/365 days per year) as requested by the project officer and in case of emergency situations.

The help desk staff shall be responsive to all SLES user requested assistance or reported problems related to the use of the network system.

The service requests may be related to users' registration, smart-card issuance or other concerns surfaced during the audits of the security and system logs. The help desk log shall be a source of information about the actual performance of the system. It must reflect not only the issues reported by the users but also the solutions and the type of actions taken.

SLES Kiosks, which are accessible by all system authorized users have similar equipment to those at individual user's desktop with certain Input/Output peripherals such as CD and DVD and floppy drives and high speed printer.

The offeror shall maintain all Kiosks (HQ and Regional) operable and respond to all Kiosks related reported problems or service requests by the users in the same way as other service request described above. A record of each service request or reported problem or incident related to Kiosk equipment must be kept in the Maintenance and Activity Log by the offeror.

The help desk staff shall manage:

- Interface with users and respond to or coordinate actions in response to users request for assistance
- Interface with ISSO, NRC Project Officers, System Administrator and other offeror resources on all operation issues.
- Coordinate activities with other NRC offices as needed as instructed by the NRC project manager.

- The help desk staff shall interface and coordinate activities with NSIR E-Safe processing center in the following areas:
    - Process all non-duplicate SGI records submitted for processing into E-Safe
    - Provide priority E-Safe support during an Incident Response while the Agency is in a Monitoring or Activation mode

C.6.6.4 System maintenance

The offeror shall maintain all SLES hardware and software on a regular basis in order to ensure continual and reliable system operation. The term "maintain" includes all activities associated with diagnostics, repair or replacement, modification or update and enhancement deemed necessary on the system hardware and software.

The offeror is required to upgrade/refresh system hardware and software to ensure appropriate maintainability and IT security controls. Hardware and software should not be allowed to become unsupported or insecure.

In the event that equipment manufacturer or vendor assistance or services may be required, the offeror must first receive approval from the NRC project manager for the intervention/service. Procurement of vendor services and all replacement parts or equipments are the responsibility of NRC. However, the offeror is responsible for providing the exact technical specifications and all other necessary information for procurement of the needed parts and/or services and keeping track of the service coverage warranties and service contract already in place or to be procured for all SLES hardware and Software.

The offeror shall maintain all servers and other equipment such as the data storage devices, infrastructure equipment (Cisco switches, Cisco Wireless LAN Controllers and Wireless Access Points) and the users' desktop and kiosk equipment.

The SLES user desktop equipment consists of a thin client terminal, and a (KVM) switch. SGI LAN Kiosks which are accessible by all system authorized users have similar equipment to those deployed at the user's desktop with certain I/O peripherals such as CD and DVD and floppy drives and high speed printer, plotter or/and scanner.

The offeror shall maintain all SLES main server room equipment, floor equipment, and desktop equipment deployed to the users. The offeror shall also maintain all other system related equipment to include the COOP and DR system and components, which are located at an alternate site.

System maintenance also includes all required activities in response to the Plan of Action and Milestones (POA&M) which are required to be completed in order to maintain the ATO for the SGI LAN and the E-Safe. The offeror shall evaluate the required actions and present a detailed execution plan for each of the actions to the NRC project manager for approval before taking the actions.

Following is the list of scheduled maintenance activities which shall be part of the offeror's responsibilities and duties under this contract:

C.6.6.4.1 Daily

The system administrator shall review all application specific logs associated with the server (i.e. IIS logs, database logs, etc.). The system administrator is considered key personnel with back up to assure duty coverage at all times.

The system administrator shall review and archive all applications security and system logs associated with the operating system. The system administrator checks for errors, warnings or other events and evaluate if the issue needs to be escalated. Additionally, the administrator shall inspect the logs for potential issues including access attempts (invalid, or valid, after-hours access) and unusual activity. Any significant findings are reported to the SLES designated NRC ISSO and the NRC Project Officer for evaluation and if necessary escalated according to the procedures outlined in the SLES Operations Manual.

In the case when logs were found to be disabled or inoperable on the system, the system must be shut down or interrupt services according to the procedures outlined in the SLES Operations Manual document. The Project Officer and the designated SLES ISSO shall be notified by the offeror before appropriate actions are taken to remedy the situation. When audit logs are returned to normal state, the system administrator may restart or resume services.

The system administrator shall review security sites for vulnerabilities: www.ciac.org, www.cert.mil, and all appropriate vendor sites. The appropriate vendor sites include all sites for both the operating system and applications that are running on the server(s). These may include www.microsoft.com, www.BEA.com and others.

The system administrator shall evaluate and apply system or application patches as appropriate. Only after NRC approval following the change control procedures in the Configuration Management Plan (CMP), the patch may be installed on the production system.

The system administrator shall monitor RAID integrity and drive availability. Any hard drives that fail will be replaced. Replacement of failed devices must follow Configuration Management procedures outlined in the system Configuration Management Plan.

The system administrator shall verify that system backups have occurred as scheduled. The administrator shall notify the NRC project manager if backups have not occurred and proceed by either running new backups immediately or troubleshooting the issue and running the backups as soon as the issue is resolved.

The system administrator shall change application passwords when any privileged users leave with NRC project manager approval.

C.6.6.4.2 Weekly

The system administrator shall update anti-virus definitions whenever new profiles become available.

The offeror assures that system backup tapes and other media not being used are stored outside of the server room and rotated on a regular basis. Specific procedures to be followed by the offeror for the handling, storage and the rotation of the backup tapes and media are outlined in the Operation Manual.

The system administrator shall monitor servers' memory storage/used disk space, and delete temp files as necessary. The system administrator shall notify the NRC project

manager if network resources are being diminished in an unusually rapid fashion or if resources are running low on any device.

The system administrator shall reboot servers (if necessary) and ensure system comes back online and operates normally.

The system administrator shall check management workstation access logs for activities and verify that the usage is not unusual.

C.6.6.4.3 Monthly

The offeror shall manage the privileged group accounts access.

The administrator shall monitor activity on user accounts and disable those user accounts that have been inactive for at least 30 days.

The system administrator shall perform a network system scan using NRC CSO scanners and analyzers, DISA Gold Standard to check for network vulnerabilities on the production servers. Any vulnerability found during a scan will be reviewed and acted upon as necessary and in the appropriate time frame according to NRC policy, and the SLES policies on Configuration Management.

C.6.6.5 Server Shutdown/Restart

The offeror shall be responsible for performing system shutdown and restart. System shutdowns may be required as a planned or unplanned event. Planned servers maintenance shutdowns and other orders may be performed providing that they are pre-approved by the NRC project manager and the NRC ISSO and at least a 24 hours notice is given to the system owner or the designee, the users and other stakeholders. Unplanned shutdown events could be the result of server failure or administration events such as virus infection, audit log failure, loss of power, or security incident investigation. In the event of a power outage, the SLES will rely on an Uninterruptible Power Supply to provide one hour of backup power. This will allow enough time for a graceful shutdown of the servers to prevent loss of information. In the case of either planned or unplanned events, daily maintenance logs must be annotated with the cause and purpose of the event. The NRC project manager and NRC ISSO must be notified in all cases of unplanned shutdown events and it will be the administrator that can authorize restart of one or more system servers.

C.6.6.6 Disaster Recovery

The offeror shall be responsible for taking the following actions in case of a partial or total interruption of the SLES system operation as a result of system equipment failure due to an unforeseen event.

The system administrator shall determine the causes and the extent of the damage to the SLES system and shall submit a remediation plan of action to the NRC project manager for approval.

The system administrator shall prepare a list of accredited hardware and software to NRC project manager for procurement. Once HW/SW is replaced or (re-)installed, the system administrator must perform all necessary functional tests to ensure that the system is functioning properly.

The system administrator, the ISSO, and NRC project manager shall determine what (if any) content on the SLES must be restored from the backup device/tape. Once the data is

restored the administrator must perform necessary test to ensure data integrity and total system restoration. The restored content is made available to the SLES users.

All backup and recovery efforts will be documented in the maintenance and activity log.

The NRC desires to improve the availability of the SLES system through redundancy and intends to develop a failover solution as resources allow. Upon request by the NRC, the offeror shall provide a failover solution for SLES. If accepted, the offeror shall maintain the failover equipment using the same standards as outline throughout this section (C.6.6).

C.6.6.7 Configuration Management

The configuration management and change control processes are documented in the SLES configuration management plan. The offeror must follow the policies and procedures outlined in this plan to record any changes in the SLES equipment baseline configuration including operating system and all applications including E-Safe servers. The ISSO is responsible for the security posture of the system. Any changes to the system security posture must be approved by the ISSO. The offeror shall not make changes to the system's security posture without the appropriate involvement and approval of the Change Advisory Board which includes NRC project manager, ISSO, and Senior Information Technology Security Officer.

The offeror shall update the SLES Configuration Management document to reflect all approved configuration changes in the SLES servers, networking equipment, controllers and users' desktop and kiosk equipment.

See section *C.5.2.3.3 Service Asset and Configuration Management* of this SOW to obtain a greater understanding of the NRC's configuration management requirements. It is expected that the assets managed under this task will be managed centrally with all of the other NRC ITI assets.

C.6.6.8 System Documentation Reference Update

The following is a short list of important reference documents that must be reviewed and updated by the offeror periodically.

1. Risk Assessment *
2. Configuration Management Plan
3. System Security Plan*
4. Operations Manual*
5. User's Guide
6. User's Desktop Reference
7. Administrator's Guide

* Safeguards Information.

The offeror shall make the necessary changes or updates to these and other existing system documentations at the request of the Project Officer. The changes or updates to these documents and other may be required as a result of system configuration changes or actions taken in response to the SLES (SGI LAN and E-Safe) POA&M's to maintain the system ATO.

Every time a change or update is to be made in an existing system document, the following steps shall be followed through by the offeror:

- Necessary changes are made in draft form
- The draft document is submitted to NRC project manager for concurrence
- NRC approved changes are added to the appropriate document

C.6.6.9 Status Meetings

The offeror shall schedule, prepare and conduct bi-weekly status meetings with the NRC SGI LAN project management team during which system operational status and the O&M tasks under contract are presented and discussed. The offeror shall produce minutes of each meeting and shall submit them within three days after each meeting to the Project Officer for concurrence.

At the request of the NRC project officer, the offeror may be requested to attend other meetings related to the operation and maintenance of the system. At a minimum, there will be one system review meeting conducted per quarter throughout the life of the contract that must be attended by the offeror.

The offeror may be requested by the Project Officer to document/produce minutes of these meetings.

Item	Deliverable	Delivery Schedule
1	Meeting minutes and presentation	Bi-weekly
2	System review report/minutes	Quarterly

Monthly Status Report

The offeror shall provide a monthly status report to the NRC project officer and the contracting officer by the 10th day of each month.

The monthly project status report must include at the minimum the following information:

1. Highlights of important activities/events which occurred during the reporting period.
2. Staffing plan and changes
3. Current tasks and deliverable status. This shall include the cumulative and current hours of each labor category spent on each task.
4. Projected activity plan for the next reporting period.
5. Up-to-date financial status to include prior, current and anticipated expenditures.

Additionally the offeror is required to produce a one page dashboard view of the SLES system status for NRC management on a monthly basis. The offeror may also be requested to produce a quarterly newsletter to communicate the status of system operation and

development/changes, deployment, and migration efforts. The offeror shall report on document count, user adoption rate, files created per month, files uploaded and retrieved per month, help desk calls and other information as requested by the project officer.

C.6.7 Technology Assessment Center

The Technology Assessment Center (TAC) Lab is used for early testing and assessing of new and emerging technologies that have not been approved for use in the NRC's production environment. Within the TAC environment, NRC customers conduct pilot studies, investigate new technologies, and identify how selected technologies might support NRC operations. After a technology has been successfully tested in the TAC, the results of that testing may be used by an NRC office to develop a business case to support further testing, and eventual implementation of that technology within the production environment. The work conducted in the TAC helps maintain and update the NRC's IT Technology Road Map for infrastructure investments and the Technology Reference Model, both of which are elements of NRC's IT planning process.

The TAC lab consists of approximately 40 devices, primarily workstations, laptops, servers and network hardware. Most workstations and servers are Microsoft Windows/Wintel based, but they also include Red Hat Linux systems as well as Cisco network infrastructure. The TAC is not connected to NRC's production environment, to ensure that testing cannot interfere with NRC's operations.

The current TAC network infrastructure includes Cisco routers and switches and a Cisco ASA 5520 firewall, network attached storage, Domain Name Server (DNS) devices, and other hardware. On the Windows Intel side, most of the machines are Intel Pentium-class running Windows XP or Windows Server 2000/2003.

Operating systems now used in the TAC include: Microsoft Windows *2000/2003/XP/Vista*, Cisco IOS, Red Hat Linux, and VMware ESX. Databases now in use are Microsoft SQL Server 2000 and 2005, although Oracle will soon be introduced. Other software and hardware used in the TAC include but are not limited to: Microsoft Office, Microsoft Active Directory, Microsoft Office Sharepoint Server, Microsoft Terminal Server, Microsoft Exchange/Outlook, Citrix MetaFrame, vmWare, Macromedia ColdFusion, Infoblox DNS appliances, Ironport mail gateways, Bluecoat proxy, Cisco ASA firewalls, Symantec Ghost, Symantec backup, Symantec Antivirus, Patchlink,. However, the NRC and the TAC environment are constantly evolving, and the TAC will continue to introduce new hardware, platforms and software applications.

The offeror shall provide all necessary personnel, labor, travel, and supervision necessary to support the activities of the TAC environment. Other IT engineers with specialized skills shall be made available by the offeror as needed. Engineers with specialized skills will be provided through T&M arrangements with the NRC under the Integration task described in the Core Services section.

The lead engineer and other offeror staff will be responsible for configuration, hardening, testing, provisioning, integration, installation, documentation, troubleshooting, operation, monitoring, security and maintenance of the networks and computers (hardware and software) in the TAC. This includes system installation, hardware/software support, problem tracking and reporting, backup, emergency planning, router and network maintenance, hardware/software inventory, tracking of software licenses and support agreements.

The lead engineer and offeror support staff shall develop and maintain documentation, procedures, inventory information, and operational plans for TAC equipment and activities.

The support shall include developing and maintaining hardware/software inventory records and documentation for individual TAC systems and network configurations. They shall support NRC in the preparation of security documentation for the TAC, and for technologies tested in the TAC. They shall prepare procedures for the operational and maintenance support of the hardware, software, and peripherals, including recordkeeping.

The support shall include, but not be limited to:

1. Network administration for TAC networks, and systems, operational and maintenance support for TAC activities;
2. Support for IT assessments, pilot studies and IT demonstrations, and assistance in the development of related documentation;
3. Configure and install IT resources in the TAC, including hardware, software (including upgrades and patches), networks and peripherals;
4. Maintain connections and cables between workstations, servers and supporting peripherals. Configure new hardware into existing IT system environment networks;
5. Install, configure, and support Cisco, Linux, and Wintel hardware, operating systems, and application software in the TAC, as well as supporting hardware such as scanners and printers;
6. Test IT installations, IT upgrades, or reconnected equipment and software in the TAC in accordance with relevant NRC IT and IT security directives and procedures;
7. Provide TAC user support associated with the use of network services, security, and Internet access, including use of FTP, Telnet, Citrix and other remote access methods;
8. Provide problem or fault identification, problem tracking, and resolution, and maintenance of TAC Linux and Wintel network infrastructure and components;
9. Assist in preparing security documentation for the TAC, and participate in security, emergency preparedness, continuity of operations and other security activities, documentation and audits for the TAC as required by NRC's IT security procedures.
10. Coordinate and assist OIS staff and other contractors in implementing connectivity initiatives and testing new versions of operating systems and hardware, software, and peripherals.
11. Develop and maintain an inventory of TAC IT hardware and software. Conduct semi-annual audits to verify inventory information.
12. Document and maintain a listing and graphical representation of the TAC IT environment.
13. Develop an archive and retrieval plan for IT system and application data backup and recovery for the TAC. Perform LAN Administration services for the TAC, including monitoring and managing file server disk space, and monthly backups.
14. Monitor IT hardware and software maintenance agreements or contracts, and track software licenses associated with the TAC.

Additional Data Center Software and Hardware:

Operating Systems

Windows 2000 Server and Advanced Server

Windows 2003 Server and Advanced Server

Windows 2003 Cluster Server

Windows 2008 Server

Windows 2008 Server with Hyper-V

Solaris 8,9,10

HP-UX 11

Red Hat Linux Enterprise Server 5

IBM OS/390

VMWare ESX 3.5

Databases

MSSQL 2000

MSSQL 2005

DB2

CA-RAMIS

Sybase 12.5

COTS Applications

MS IIS 5 and 6 web server

PeopleSoft 7.6 and 8.9

SunOne Web Server (Iplanet)

Apache Web Server

MS Sharepoint Enterprise 2007

MS Project Server 2007

MS Biztalk 2006

Macromedia Cold Fusion MX

Filenet Panagon Content Services

Filenet Panagon Web Publisher

Filenet Web Services

Citrix MetaFrame

Convera RetrievalWare

Jboss

Tuxedo

WebLogic

Lotus Notes

Crystal Reports Enterprise

Avepoint

WebTrends

Symantec Enterprise Virus Server

NetApp ReplicatorX

AINS FOIA Xpress

IBM Rational Suite

Suresync

Veritas Volume Manager

Tivoli Storage Manager

Tivoli Workload Scheduler

IBM Rational ToolSet

MS Visual Source Safe

Documentum Foremost

StorageTek ACSLS

WSFTP Server

WSFTP FTP Sync

RACF

X-Windows

TSO

WYLBUR

Voyager

AnyQueue

VPS (VTAM Printer Support)

NIH SILK WEB

Tools

Unix shell scripting

PERL scripting

Whats Up Professional

Visual Basic scripting

WinBatch scripting

Window command scripting

SSH

SFTP

MS Baseline Analyzer

DISA Gold Disk

Nessus scanner

CIS Security scoring tools

HTML editors

Patchlink

Microfocus COBOL

Symantec Backup Exec System recovery Server

Hitachi DAMP

Hardware

Hitachi 9500 series Disk Arrays

NetApp FAS Disk array

Brocade Fiber Switches

StorageTek Tape Libraries

HP Proliant series servers Intel based servers

Dell PowerEdge series servers Intel based servers

Sun V200 and V400 series SPARC based servers

HP 9000 series RISC based servers

F5 load balancers

Cisco 11501 load balancers

HP MSA storage units

Dell PowerVault storage units

C.6.8 Emergency Response Data System (ERDS) Operations and Maintenance

This section describes the specific requirements, using the NRC ITISS contract vehicle, for operations and maintenance of the Emergency Response Data System (ERDS) solution to authorized NRC Headquarters and regional users and evaluates external access policies and procedures for access by Federal, State and local agencies, and Licensees.

C.6.8.1 General

The Emergency Response Data System is one of the Information Technology (IT) systems that are used in the Operations Center after a nuclear emergency is declared at a U.S. nuclear plant. The system is Federally Regulated through 10 Code of Federal Regulations (CFR) 50.72.A.4, which states that the licensee must activate ERDS within one hour after the licensee declares an emergency at an emergency class level of "alert" or higher (higher means the declaration of a "site area emergency" or "general emergency"), and it is a system that is designed to collect nuclear plant performance and environmental data for analysis by NRC and State emergency response personnel. ERDS is also used in the HOC at times when the NRC and licensee participate in planned drills.

ERDS is currently implemented at NRC Headquarters (HQ), the four (4) NRC Regions, the NRC Technical Training Center (TTC) and is used over the web by twenty-two (22) States who qualified to use ERDS because their State boundary falls within the 10-mile Emergency Protective Zone (EPZ) of a specific plant or group of plants and they have signed a memorandum of understanding (MOU) with the NRC. Additionally, NRC modems are installed at every operating nuclear power plant in the country (65 plants, 104 units) so that the required ERDS data can be transmitted.

During declared emergencies and planned drills, the ERDS receives an automated feed of digital data from nuclear power plant operators over long distance analog telephone circuits. The type of information sent by the nuclear power plant allows the NRC to assess the overall adequacy of licensee actions, provide recommendations for mitigating accident consequences and to protect the public. Data such as system temperatures, pressures, water levels, flows, radiation levels, wind speed and direction are all transmitted by the plants.

The offeror shall maintain continuous availability of key personnel who are required to successfully perform the work required in this statement of work. The offeror shall ensure that both key and backup personnel are committed in performing these services during the NRC's official hours of operation and shall provide a minimum one (1) hour response to any NRC calls during all other times.

The offeror's personnel shall adhere to and implement all documented required security measures in their activities as set forth by the Federal Information Security Management Act (FISMA) throughout the life of the contract. The offeror shall maintain the ERDS System Security Plan and develop any other type of system security and operational documentation as requested by the NRC Project Officer.

The offeror shall adhere to and apply the NRC Project Management Methodology (PMM – see MD 2.8) Operations and Maintenance (O& M) phase throughout the life of the contract. The PMM provides important system development guidance for all NRC IT programs across the life cycle from initial concept to retirement and defines key milestones, activities and deliverables.

The offeror shall coordinate their activities with other NRC internal offices, such as, the Office of Information Services (OIS) and the Office of Administration (ADM). In doing so, the offeror may be required to work with various NRC staff and other contractors subject to technical direction by the NRC Project Officer for this contract.

In case of emergencies or for reasons related to system repair/maintenance, the offeror may be called or required to work outside of the regular hours of operations as mentioned above.

In addition, the offeror shall:

1. Maximize the availability of the Emergency Response Data System (i.e. minimize the length and frequency of service outages);
2. Minimize the time from when a service request is initiated, to when the offeror responds to that request;
3. Minimize the discrepancy between date of a given scheduled system backup and date on which that system backup occurs; and,
4. Minimize the time from when an unusual file storage growth pattern is identified to when the appropriate staff members are notified

C.6.8.2 Monitoring

The offeror shall monitor the daily performance of the ERDS hardware and software to identify and resolve hardware problems that may arise. The offeror shall monitor the performance of the physical equipment each day and look for any unusual activity that may represent potential threats, introduce adversity or degrade system performance. The offeror shall notify the NRC project officer about any problems identified and obtain approval from the NRC project officer before resolving them. The term "ERDS hardware" and "ERDS Software" includes all of the materials listed below.

Primary, Secondary and Development ERDS Servers

Dell Computers PowerEdge 6850 (7)

Interface Nodes/Domain Servers

Dell Computers PowerEdge 2950 (3)

Web Servers

Dell Computers PowerEdge 860 (2)

Workstations

Dell Computers Optiplex 745 (2)

Tape Library with Autoloader

Dell Computers PowerVault 124T (2)

Color LaserJet Printer

- Dell Computers 3115N (1) and 3010N (1)

Network Switch

- Dell Computers PowerConnect 2724 (2)

Integrated Services Router

- Router Cisco 3825 (2)
- Power Supply PWR 675-AC-RPS-N1 (2)

Universal Power Supply

- APC Smart-UPS 5000 with transformer (2)
- APC Smart-UPS 5000 (1)
- APC Smart-UPS 3000 (1)

Rack

- Dell 42U Rack (4)

Keyboard Monitor Mouse (KMM) console

- Dell 15 inch rack mount console (3)

CISCO

- ASA5510 (4)
- ASA5505 (71)
- Unmanaged Switch

Microsoft Windows 2003 for servers

Microsoft Windows XP

Microsoft (IIS) Internet Information Services 6.0

Microsoft Visual Studio MSDN Profession Subscription

Microsoft SharePoint Services 2007

Microsoft ASP.Net 2.0

Microsoft SQL Server 2005

Microsoft Office Basic Edition 2003

Symantec Backup Exec 11d

Symantec Norton Anti Virus

OSIsoft PI Suite 3.4

- PI Server
- PI Interface

IT Monitor

RTWebParts

The offeror shall be required to update the ERDS hardware and software list of this contract, within 30 days, when additions and/or deletions are made to the ERDS hardware and software list. Upon revision of the hardware and software list, a copy shall be provided to the NRC Project Officer for a potential contract modification.

The offeror shall maintain a proactive security stance by accurately documenting routine and non-routine actions occurring on the system in the ERDS Maintenance and Activity log. The offeror shall document all abnormal system malfunctions in the log. At a minimum, the information recorded in the ERDS Maintenance and Activity log shall include the name of the affected device(s), the name of the offeror's staff member making the entry, the date of the malfunction, details about the abnormality, any actions taken by the offer's staff member to remedy the situation, and whether or not further action is still required.

The offeror shall ensure that only authorized personnel are included in the privileged accounts and monitor activity on user accounts. The offeror shall change application passwords anytime a privileged user permanently stops using ERDS.

The offeror shall verify that the management workstation anti-virus definition files are up-to-date.

The offeror shall issue, monitor and control all system certificates required for ERDS web access.

The offeror shall review security sites for vulnerabilities: www.ciac.org, www.cert.mil, and all appropriate vendor sites. The appropriate vendor sites include all sites for both the operating system and applications that are running on the server(s). These may include www.microsoft.com, and others. The offeror shall also evaluate and apply system or application patches as appropriate. Only after approval following the change control procedures in the NSIR Change Advisory Board charter, the patch may be installed on the production system.

The offeror shall monitor RAID integrity and drive availability. Any hard drives that fail shall be replaced.

The offeror shall apply routine plant data point changes on all systems installed at Headquarters and Region IV as needed to ensure data integrity. These changes are issued by licensees and are unique to the nuclear plant.

The offeror shall conduct data transmission tests with the nuclear units at each nuclear plant in the United States per quarter to verify the integrity of the communications link between NRC and the nuclear plant. As a rule, every plant must be successfully tested once in every quarter throughout the life of the contract. Also, each plant test that is conducted by the offeror in any given quarter throughout the life of the contract is not considered complete until the plant test is fully successful. The tests shall be conducted at selected plants each week, based on the schedule of testing provided by the NRC, between Tuesday and Thursday 8:00 A.M. to 4:00 P.M. EST (Monday and Friday shall be reserved for re-testing, if that is needed), ensuring that each plant is tested once per quarter.

The offeror shall maintain a quarterly testing log to document the details about each test conducted in a given quarter. At a minimum, the log shall contain the name of the individuals contacted at each facility, the date and time they were contacted and the scheduled date that the test will be conducted.

C.6.8.3 Maintenance

The offeror shall maintain the ERDS hardware and Software on a regular basis to ensure continual and reliable system operation. The term "maintain" includes all of the various activities associated with repair, modification, and enhancement of the ERDS hardware. The term "ERDS hardware" and "ERDS Software" includes all of the materials listed in Section *C.6.9.2 User Support*.

The offeror shall also regularly review information provided by each of the ERDS software manufacturers about potential problems and apply corrective software updates once approval is given by the NRC Project Officer.

The offeror shall maintain operability of the ERDS hardware and software required for the successful reception, storage, use and retransmission of ERDS data provided by each plant.

The offeror shall maintain operability of the ERDS hardware and software for the successful storage of ERDS data.

The offeror shall evaluate current ERDS display screens to ensure user-friendly interfaces and make recommendations to the NRC project officer for improvements. Once the NRC project officer approves the recommendations issued by the offeror and the contract is modified (if required), the offeror shall update the display screens.

The offeror shall maintain and update the ERDS user interface software including the operability of the software which provides the capability to display ERDS data in the NRC Operations Center, located in Rockville MD., as well as at the Regional Emergency Response Centers, at site team locations (nuclear power plant sites), and other locations (State Government emergency response facilities, Regional Offices located in King of Prussia, PA, Atlanta, GA, Lisle, IL, Arlington, TX, and the Technical Training Center in Chattanooga, TN) in accordance with the design specifications contained in the references listed in the Reference Materials section of this statement.

Any changes to the ERDS that are approved by the NRC project officer and instituted by the offeror shall be implemented in such a manner as not to disrupt ERDS operability with all of the existing plants.

The offeror shall follow-up with licensees on the ERDS quarterly test results to ensure adequate resolution of all identified problems.

The offeror shall maintain the development system that replicates ERDS and that shall allow for a platform for software development and troubleshooting for ERDS as required.

The offeror shall provide adaptive maintenance (software/hardware enhancements) for ERDS via contract modification. Adaptive Maintenance requests will only be issued to the offeror on an ad-hoc basis using the Agency's standard change management process.

The offeror shall maintain an operational set of twelve (12) spare plant modems, to resolve reported modem hardware failures at nuclear plants. The NRC project officer will physically provide the offeror with the analog modem pool, which currently contains six (6) of the required twelve (12) modems to maintain. As the Phase II transition continues the remaining

six VPN modems will be procured and physically provided to the offeror, ensuring there are always 12 spare modems available.

The offeror shall produce daily incremental tape backup of all the ERDS servers and a full backup once a month. The offeror shall be responsible for managing the rotation (shipping and receiving) of the backup tapes to a geographically remote NARA location from the NRC Headquarters for storage.

The offeror shall ensure that the data is recoverable from the backup tapes. The offeror shall perform verification tests to restore several different files from the tapes to temporary directories on various servers. Temporary files will be deleted after verification is complete. Verification tests of the backup system must be performed at least semi-annually and shall be documented in the Maintenance and Activities log. Procedures for data recovery "verification" test shall be edited and presented by the offeror to the ERDS ISSO for approval.

The offeror shall maintain an activity log for the ERDS portal. The offeror shall review the audit logs located in the Audit Manager of the Administration console weekly and initial the audit log each week indicating that the logs have been reviewed. The offeror shall look for any unusual activity, in particular denied logins, review the issues with the ERDS ISSO and escalate as necessary.

The offeror shall maintain the list of ERDS active users; administer registration of the new users and the removal or inactive users. In conformance with NIST standards, SP 800-53, separation of duties through system access authorization must be assured between a system administrator and a system security administrator. The administrator shall issue, monitor and control all 128 bit encrypted Secure Socket Layer (SSL) assigned certificates required for ERDS web access.

The offeror shall work on all required activities in response to the ERDS Plan of Action and Milestones (POA&M) in order to maintain an Authority-to-Operate (ATO) for ERDS. The offeror shall evaluate the required level-of-effort for performing the requested actions in the POA&M and present it to the Project Officer for approval before taking action on them.

The offeror shall apply routine plant data point library (DPL) changes on all systems installed at HQs and Region IV on an as-needed basis throughout the life of the contract to ensure data integrity. Data points are tags associated with the nuclear unit equipment at the licensees (e.g. water pumps, steam generator, wind speed, etc). These tags are replicated in ERDS as graphical display of the equipment. The changes are issued by licensees and will be provided to the offeror by the NRC PO at an estimated frequency of four per quarter. The offeror shall successfully test and document the test results in a test environment prior to deploying changes to the ERDS production environment. The offeror shall also update the DPL Test Plan whenever a change is made.

Disaster Recovery

The offeror shall be responsible for taking the following actions in case of a partial or total interruption of the ERDS system operation as a result of system equipment failure due to an unforeseen event.

The offeror shall determine the causes and the extent of the damage to the ERDS system and submit a remediation plan of action to the NRC Project Officer.

The offeror shall prepare a list of accredited hardware and software and provide it to the NRC Project Officer for procurement. Once HW/SW is replaced or (re-)installed, the offeror shall perform all necessary functional tests to ensure that the system is functioning properly.

The offeror and NRC Project Officer shall determine what (if any) content on the ERDS must be restored from the backup device/tape. The offeror shall restore the data determined to be restored. Once the data is restored, the offeror shall test the data to ensure proper data restoration.

The restored content shall be made available to the ERDS users.

All backup and recovery efforts shall be documented in the ERDS maintenance and activity log.

C.6.8.4 Management

The offeror shall maintain continuous availability of all key personnel who are required to successfully perform the work required in the SOW. The offeror shall ensure that both key and backup personnel are committed in performing these services during the NRC's official hours of operation (7:00 A.M. - 4:30 P.M., EST, Monday through Friday, except Federal holidays) and shall provide a minimum one (1) hour response to any NRC calls during all other times.

The offeror shall attend system review meetings throughout the life of the contract to discuss issues concerning things like project schedule, budget, resources, equipment, goals, milestones, or anything else that may need attention by the NRC project officer or the offeror. The frequency of these meetings will be agreed upon by both the NRC project officer and the offeror immediately following contract award. However, at a minimum, there will be at least one system review meeting conducted per quarter throughout the life of the contract. Generally, these meetings will be conducted as teleconferences.

The offeror shall provide monthly technical progress reports to the NRC project officer throughout the life of the contract to describe, in detail, the project's prior month activities. This report will provide details about both the project's technical and budgetary performance.

The offeror shall physically visit the ERDS Region 4 backup site twice annually, in order to assess and adjust the equipment as necessary. The offeror shall provide a site visit summary report to the NRC project officer. This report will provide details on the condition of the equipment and make recommendations.

The offeror shall support all of the existing security documentation and testing requirements for ERDS as set forth by the Federal Information Security Management Act (FISMA) throughout the life of the contract. The offeror shall maintain the ERDS System Security Plan and develop any other type of system-related documentation as requested by the NRC project officer.

The offeror shall maintain and revise the ERDS System Administrator Manual, the OS Configuration Guide, the ERDS Configuration & Installation Guide, the ERDS User's Manual, and all existing system drawings. The documentation of all software shall be in accordance with the criteria described in NRC Management Directive 2.8.

System Documentation Reference and Update

The offeror shall make the necessary changes or updates to existing system documentations at the request of the Project Officer. Some of these changes or updates may be as a result of required system configuration changes or actions taken in response to the ERDS POA&M in order to maintain the system ATO.

Every time a change or update is to be made in an existing system document, the following steps shall be followed through by the offeror:

1. Necessary changes are made in draft form
2. The draft document is submitted through NRC concurrence
3. Approved changes are added to the appropriate document

The offeror shall perform work under this contract in such a manner to assure ERDS availability according to the service level requirements in Appendix A: SM-SLA-23: *Emergency Response Data System (ERDS) Operations and Maintenance*. ERDS availability will be evaluated by NRC every month using the monthly technical progress reports provided by the offeror. Failure to meet this performance standard once during any given quarter throughout the life of the contract will result in the issuance of an unsatisfactory performance evaluation report by the NRC project officer.

ERDS availability shall be defined as:

$$\frac{\text{System operable time}}{\text{System operable time} + \text{System inoperable time}}$$

This formula shall be provided by the offeror in the last monthly technical progress report of each quarter.

ERDS shall be considered operable any time the ERDS hardware and software performs the following core functions:

1. Receive data from up to twenty-four reactor units simultaneously
2. Store all received power plant data
3. Support display of all plant data using the NRC approved user interface
4. Archive nuclear power plant data for further review

ERDS shall not be considered inoperable when the cause for the system failure is outside the scope of this contract (e.g., extended power failure or loss of telephone service).

C.6.8.5 ERDS Phase II Support

The offeror shall maintain the second phase solution produced through the ERDS Modernization project. In addition to all of the tasks described in this scope of work, once the second phase solution of the ERDS Modernization project is completed, the offeror shall provide the following maintenance support services associated with maintaining a new communications network for ERDS:

The offeror shall provide network support services twenty-four hours/day, seven days/week. Tasks shall include monitoring the operational state of the network, resolving any

communication problems, continuous automated tracking and daily reporting on the condition of the network to the NRC Project Officer, and providing maintenance and support services that may be necessary for all other service contracts associated with operating the ERDS network.

C.6.8.6 Reporting

The offeror shall schedule, prepare and conduct a monthly status meeting with the NRC ERDS project management team during which status and progress made in implementing the tasks under the contract are presented and discussed. The offeror shall produce minutes of each meeting and shall submit them within three days after each meeting to the Project Officer for concurrence.

At the request of the Project Office, the offeror may be requested to attend the projects team meetings, system review and other technical meetings pertinent to the ERDS Operations and Maintenance. At a minimum, there will be one system review meeting conducted per quarter throughout the life of the contract that must be attended by the offeror.

The offeror may be requested by the NRC Project Officer to document/produce minutes of these meetings.

See sections *C.5.2.5.1 Centralized Reporting* and *Appendix E: Reporting Requirements* for a greater understanding of NRC's general reporting requirements.

Monthly Status Report

The offeror shall provide a monthly Technical Progress Report to the NRC Project Officer and the Contracting Officer by the 7th day of each month. The monthly Technical Progress Report must include at the minimum the following information:

1. Highlights of important activities/events which occurred during the reporting period.
2. Staffing Plan and changes
3. Current tasks and deliverable status. This shall include the cumulative and current hours of each labor category spent on each task.
4. Projected activity plan for the next reporting period.
5. Up-to-date financial status to include prior, current and anticipated expenditures.

C.6.8.7 Training

The offeror shall provide ERDS User training when requested by the NRC Project Officer. Each training session shall consist of up to eight (8) hours of training for up to twenty-five (25) individuals, up to ten (10) ERDS operators and up to fifteen (15) State ERDS operators from the affected region. The offeror shall provide an estimated total of six (6) training sessions per year: one (1) at each of the following:

1. NRC Operations Center - Headquarters (Rockville, MD.)
2. Regional Offices (I - King of Prussia, PA; II - Atlanta, GA; III - Lisle, IL; IV - Arlington, TX)
3. Technical Training Center (Chattanooga, TN)

The contactor shall provide training materials and formal completion certificates for all training sessions provided. NRC offices will be given the option to conduct training at their location each year. The offeror shall be required to also provide up to twelve (12) two-hour webinar training session annually whenever requested by the NRC Project Officer.

C.6.9 Secure LAN and Electronic Safe

This section describes the specific requirements, using the NRC ITISS contract vehicle, for implementation and rollout of the Secure LAN and Electronic Safe (SLES) records and document management solution to authorized NRC Headquarters and regional users and evaluates external access policies and procedures for access by Federal, State and local agencies, and Licensees.

C.6.9.1 General

The Electronic Safe (E-Safe) application operates as a Major Application and is connected to the SGI LAN. E-Safe provides fully featured electronic document and record management functionality to users with secure access authorization. Management of user and group accounts are provided as an Administration services capability.

This task consists of, but not limited to, daily system and security administrative activities, tasks and activities for maintaining the E-Safe records and document management and operational users support. During the life of this contract, NRC continues to further develop and gradually deploy SLES to users in the Headquarters and regions; and eventually to all other authorized users in Federal, State and local agencies, and Licensees. The offeror shall provide O&M support services for the SLES deployment to approximately 1,000 users by the end of the contract period.

The offeror shall ensure that both key and backup personnel are committed in providing operations and maintenance support services between 7:00 A.M. and 5:00 P.M., EST, Monday through Friday (with the exception of Federal holidays). All service requests (telephone call, email, or other means of communication) must be responded to by the offeror within a 60 minute time-frame from the time that the service request was received.

In case of emergencies or for reasons related to system repair/maintenance, the offeror may be called or required to work outside of the regular hours of operations as mentioned above.

In addition, the offeror shall:

1. Maximize the availability of the Electronic Safe Application (i.e. minimize the length and frequency of service outages);
2. Minimize the time from when a Fulfillment of Service request is initiated, to when the offeror responds to that request;
3. Minimize the discrepancy between date of a given scheduled system backup and date on which that system backup occurs; and,
4. Minimize the time from when an unusual file storage growth pattern is identified to when the appropriate staff members are notified.

Records/Documentation Administration

The offeror shall provide records management and administrative services related to the use of Documentum. The offeror shall work closely with the NRC's project manager to determine

and implement the appropriate changes and enhancements to the E-Safe application. The offeror shall also maintain proper set-up and disposition of retention schedules for the E-Safe records in accordance with the NRC's NARA-approved schedules, and NRC Records Management policies.

C.6.9.2 User Support

C.6.9.2.1 Access

The offeror's designated security administrator shall administer user registration (addition and removal of users) based on established procedures outlined in the SLES Operations Manual. The offeror must also maintain an active SLES user list. . This activity includes set up and removal of the SLES user desktop equipment. In conformance with NIST standards, SP 800-53, separation of duties through system access authorization must be assured between the system administrator and the system security administrator who is in charge of access card issuances/cancellations and the system access control administration.

C.6.9.2.2 Helpdesk Support

The offeror shall provide help desk services during the normal business hours of Monday through Friday, 7 a.m. to 5 p.m. (EST) through the NRC established phone number and email with dedicated on site staff. The offeror may be asked to support users at anytime after the business hours as requested by the project officer and in case of emergency situations.

The help desk staff shall be responsive to all SLES user requested assistance or reported problems related to the use of the E-Safe system.

The service requests may be related to users' registration, smart-card issuance or other concerns surfaced during the audits of the security and system logs. The help desk log shall be a source of information about the actual performance of the system. It must reflect not only the issues reported by the users but also the solutions and the type of actions taken.

The help desk staff shall manage:

1. Interface with users and respond to or coordinate actions in response to users request for assistance
2. Interface with ISSO, NRC Project Officers, System Administrator and other offeror resources on all operation issues
3. Coordinate activities with other NRC offices as needed as instructed by the NRC project manager.

C.6.9.3 Records/Document Management

The help desk staff shall provide Records/Document Management support for users using EMC's Documentum product. The offeror shall assist and train users with general use of the applications and troubleshoot specific reported issues related to records/document management. The offeror shall support users with up-loading, down-loading, retrieving documents, and setting up workflows.

The help desk staff shall interface and coordinate activities with NSIR E-Safe processing center in the following areas:

1. Process all non-duplicate SGI records submitted for processing into E-Safe

2. Provide priority E-Safe support during an Incident Response while the Agency is in a Monitoring or Activation mode

SLES Kiosks, which are accessible by all system authorized users have similar equipment to those at individual user's desktop with certain Input/Output peripherals such as CD and DVD and floppy drives and high speed printer.

The offeror shall maintain all Kiosks (HQ and Regional) operable and respond to all Kiosks related reported problems or service requests by the users in the same way as other service request described above. A record of each service request or reported problem or incident related to Kiosk equipment must be kept in the Maintenance and Activity Log by the offeror.

C.6.10 Development Facility

New IT applications and systems are regularly brought into the NRC production environment. These can be either custom developed or commercial-off-the-shelf solutions. Many of these systems are developed by third-party contractors who know very little about the NRC ITI. Currently, development environments are set up completely externally to the NRC, and it is only at the test stage that system integrators encounter problems related to bringing their systems into the NRC ITI production environment.

Therefore, the offeror shall provide a development environment for developers and/or system integrators to work in which is separated from the production environment. This development environment must replicate the actual production environment so that development issues can be resolved early and real problems can be identified and corrected. Although individual IT system owners must take the responsibility to move their systems through this process, the offeror shall help them to succeed in this endeavor.

Development Management – The offeror shall provide the technical environment for and maintain the ability to develop new applications and hardware to ensure a smooth transition into the NRC ITI.

In addition, the offeror shall:

1. Maintain the development environment network including infrastructure, servers and applications with up to date patching at the same level of the NRC ITI;
2. Ensure that the development environment is segregated from the production environment;
3. Operate and manage the development environment to support application development, network performance impact analysis, network modeling and simulation, integration, demonstration, product briefings, evaluation and orientation/training for COTS and custom services and applications to be integrated into the infrastructure;
4. Ensure application and hardware integration into production without adverse impact on the infrastructure;
5. Provide non-production data sets for development systems. No production data shall be used in the development environment; and,
6. Manage a schedule of development environment availability, publish that schedule, and work with customers in scheduling the use of the environment.

C.6.11 Microsoft SharePoint Support

The NRC SharePoint program structure consists of several components designed to support the SharePoint technical environment, extend SharePoint to serve business needs, and educate and support users so that they can leverage SharePoint features.

A few of these components that are integral to the success of this task include:

SharePoint Program Management – is responsible for developing and implementing the SharePoint vision using the resources available to the program and for compliance with applicable IT/IM/information security regulations and requirements. The SharePoint vision supports and complements the ECM program vision. The NRC SharePoint Manager for this contract is part of the SharePoint Program Management.

Project Teams – are temporary, integrated teams responsible for rolling out SharePoint and for delivering a unique SharePoint product or service. Project teams are lead by NRC project managers using the NRC Project Management Methodology (PMM) and the SharePoint extensions to manage the project.

SharePoint Administrators – a permanent team serving as a forum for knowledge exchange between Primary SharePoint Site Administrators. Initially, the team will consist of Office level Primary Site Administrators, but will expand to division-level Primary SharePoint Site Administrators over time. The NRC end user will first contact their respective SharePoint Administrator for support. If their SharePoint Administrator is unavailable or is unable to adequately address the end user's need, the end user will then call the Tier I Help Desk for support.

The offeror shall provide NRC Microsoft SharePoint end users with Tier I Help Desk support. At a minimum, the offeror shall:

1. Provide Tier I Help Desk support to NRC MS SharePoint end users on the 18 out-of-the-box features.
2. Utilize the NRC service desk tracking system (provided under the Core task) to track requests and ensure that all requests for service and problems are responded to in a timely manner and properly closed out in the tracking system when completed.
3. Address end user questions concerning the features, functions, and operation of MS SharePoint. The offeror shall make a first attempt to resolve the end user's SharePoint problem directly over the phone. The Help Desk staff member shall apply remote Service diagnostics to try to resolve the request directly if possible. If not, the request will be dispatched for face-to-face resolution.
4. Develop and maintain MS SharePoint Help Desk support policies, procedures, and practices as needed.
5. Develop and maintain MS SharePoint training guides and support materials as needed.
6. Track and maintain Help Desk metrics for inclusion in the Help Desk Metrics Report. The NRC SharePoint Manager and the offeror shall agree on the type of metrics to include in the report.

7. Develop an electronic End User Survey to gauge customer satisfaction with the MS SharePoint Help Desk. A Help Desk Survey Results Report shall be developed to include the survey results.
8. Coordinate with the NRC Customer Support Center on issues related to NRC MS SharePoint.

C.6.11.1 Deliverables

Item	Deliverable	Due Date
1	Support Policies, Procedures, and Practices	As needed
2	Training Guides and Support Materials	As needed
3	Help Desk Metrics Report	Bi-weekly
4	End User Survey	Once per quarter
5	Help Desk Survey Results Report	Once per quarter

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

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

In the event the offeror anticipates difficulty in complying with the delivery schedule, the offeror shall immediately provide written notice to the Contracting Officer and NRC SharePoint Manager. Each notification shall give pertinent details, including the date by which the offeror expects to make delivery; provided that this data shall be informational only and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule.

Each deliverable shall first be submitted in draft to the NRC SharePoint Manager for review. NRC shall have 10 business days to review each draft deliverable and respond with comments or approval. If more time is required, the offeror will be notified by the NRC SharePoint Manager.

If revisions are required, the offeror has 5 business days to complete the revisions and submit the revised draft deliverable to the NRC SharePoint Manager. For each deliverable (draft or final), the offeror shall provide one (1) electronic version of the deliverable via e-mail to the NRC SharePoint Manager, unless otherwise indicated. 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.

Unless otherwise specified, all deliverables developed under this task must be formatted in Microsoft Word or Microsoft Excel (version 2003 or later version as approved by the NRC SharePoint Manager).

The NRC shall work with the offeror to define specific quality standards for each deliverable. The NRC expects the deliverables to be timely, thorough, and accurate. The deliverables shall be submitted to the NRC SharePoint Manager on or before the scheduled due date; completely address the NRC's requirements; be free of formatting and spelling errors; be clearly written; and have no incomplete sections. As each deliverable is usually the end result of a series of activities, prior to starting on each task, it is vital that the offeror and the NRC agree on the approach for the deliverable, the activities involved to develop it, and expectations for the final product.

C.6.11.2 Ad-Hoc Meetings

The offeror shall be available to attend Ad-Hoc meetings in person requested by the NRC SharePoint Manager. The offeror will be given 24 hours notice before an Ad-Hoc Meeting will be convened.

C.6.12 Extraordinary Move Support

From 2013 – 2015, the NRC will centralize all headquarters staff not currently located in One White Flint North or Two White Flint North into a new building in Rockville, Maryland. The NRC anticipates 1500 staff moves in 2013, and 6000 extra staff moves in each of 2014 and 2015 to achieve the consolidation (some people will be moved more than once). These moves are in addition to the current average annual moves of 1000. The offeror shall bid two separate optional tasks to support the extraordinary moves.

In the first task, the offeror will support the approximate 1500 moves to the planned building located adjacent to the main headquarters building at 11555 Rockville Pike, Rockville from the current four headquarters buildings at 6003 Executive Boulevard, Rockville, MD; 7201 Wisconsin Ave, Bethesda, MD; 12300 Twinbrook Parkway, Rockville, MD; and 21 Church Street, Rockville. The offeror shall move all computer equipment (including GFE equipment) within a short time frame (4-8 weeks). These moves could occur as early as 2012.

The second task will support approximately 6000 moves over a multi year period. These moves will not occur until the first task above has been completed. The offeror shall move groups of staff from either 11545 Rockville Pike or 11555 Rockville Pike to 21 Church Street, Rockville in phases while the existing office space is being renovated. The offeror shall then move those staff back to their renovated offices. Then, the offeror shall move another group of several hundred staff until the renovations are complete. The offeror shall move all computer equipment (including GFE equipment) for each move within a short time frame (2-4 weeks). These moves could occur as early as 2012 and may occur during the entire period of performance of the contract.

C.7 TRANSITION CONSIDERATIONS

C.7.1 Initial Transition

Within their bid, the offeror shall provide a detailed schedule for how they intend to assume management of the NRC ITI, including:

1. providing adequate security cleared staff
2. transfer and/or procurement of ITI components
3. management tools (software, etc.) procurement, installation, and training
4. transfer of ongoing integration projects from the incumbent ISSC contractor

The current environment is a mix of assets leased by the incumbent ISSC contractor, assets owned by the incumbent ISSC contractor, and assets owned by the Government. The majority of the assets in the core tasks are leased by the incumbent ISSC contractor. The incumbent ISSC contractor estimates that they own 1/3 and lease 2/3 of all equipment provided to the NRC under their contract. Further, the incumbent ISSC contractor values the 1/3 of owned equipment between $3,000,000 and $4,000,000.

The incumbent ISSC contractor will, upon award of the ITISS contract, provide a report of all assets that make up the ITI, designating if they are leased or owned. The offeror will perform a physical inventory and inventory valuation within sixty (60) days of Contract award.

It is anticipated that the new Contract and the current Contract will overlap for 180 days. The offeror will use the first 90 days of this period to prepare for the transition (inventory, hiring, security clearances, etc.) and the remaining 90 days will be to transition infrastructure services from the incumbent ISSC contractor.

Two equipment leases will extend into the initial year of the base period for the ITISS contract. One additional lease will extend several years into the base period of the ITISS contract (see Table 4 – Existing Equipment Leases That Extend into ITISS Contract Base Period, below).

Qty	Manufacturer	Description	Term (Mos.)	Lease End Date
1	Cisco	WS-C4506 S2+96 (Catalyst 4500 6-slot chassis bundle)	36	6/30/2011
50	Dell	Latitude D630 C2D/2.2GHZ		
250	Dell	Optiplex 755 C2D/2.66G DT		
2750	Dell	Optiplex 755 C2D/2.66G DT	36	8/31/2011
1500	Dell	Optiplex 760 C2D/2.0G DT	36	12/31/2012
600*	Dell	Latitude E6400 C2D/2.8G		
200*	Dell	Latitude E4300 C2D/2.53G		

* The precise quantity of laptop computers was unknown at the time of RFP release, so approximations are provided

Table 4 – Existing Equipment Leases That Extend into ITISS Contract Base Period

The Offeror shall choose one of two options in how to manage these existing leases: 1. The Offeror can negotiate and assume these leases with the hardware leasing company and

complete the term of each lease; or, 2. The Offeror can terminate these leases and absorb the termination cost in their proposal cost.

The incumbent ISSC contractor may still be utilizing other leased equipment at the time of ITISS contract transition. The Offeror will also have the option of transferring these leases as well. These leases will be for beyond the current 36-month term of the original lease.

Upon award of the ITISS contract, the offeror will select the assets to be purchased from the incumbent ISSC contractor. For the valuation of owned assets being transferred from the incumbent ISSC contractor to the offeror, a formula has been established. This formula takes into account the age of the equipment and the Government's monthly cost. Upon legal transfer of the assets from the incumbent ISSC Contractor to the offeror (no more than 90 days after notice to proceed with the new ITISS contract), the incumbent ISSC Contractor's responsibility for ITISS services shall terminate. All incumbent existing assets should be less than three (3) years old unless the asset has a demonstrable ongoing life or the life has been extended at the request of the NRC.

The offeror shall be responsible for all costs associated with providing, maintaining, and operating the NRC ITI. All costs of inventory and transfer will be the responsibility of the offeror.

C.7.2 Other Transition Considerations

The NRC will, at all times, retain the ownership of any data provided by the Government to the offeror during the period of performance of the ITISS Contract. At the expiration of the contract and at any point during the contract, the offeror shall provide the NRC with all data in an easily portable format that maintains any relational information.

C.7.3 Transfer of End User Assets to a Successor Offeror or the Government

The offeror will propose an asset transfer plan to be enacted at the end of the ITISS contract. The offeror's proposed Transition-out Asset Transfer approach shall specify the transfer of assets back to the Government or successor offeror using a comparable wholesale market value basis upon termination or expiration of the Contract and transfer of leases on leased equipment as requested. The plan will state that the successor offeror will have the option to select assets for transfer.

Upon expiration of the ITISS contract, the offeror shall transfer ownership of all installed hardware, software, maintenance agreements, operational data (including CMDB data, incident data, and known error/knowledge data), and associated documentation to the Government or successor offeror. This transfer shall be accomplished in accordance with terms and conditions mutually agreed to upon award, and utilizing an independent third party valuation. In no case shall the asset transfer cost exceed the current wholesale market value of the installed assets as established by an independent third party.

All leased or owned assets that are not selected for transfer will be the responsibility of the offeror. Under no circumstances will the NRC or the successor offeror be liable for any leases extending beyond the end of the contract, or for disposal of the assets.

C.8 KEY PERSONNEL

Resumes shall be provided for any Key Personnel or their replacements. The offeror must demonstrate that the qualifications of the prospective Key Personnel are adequate to meet the requirements of this Contract. The offeror must demonstrate that the qualifications of replacements personnel are equal to or better than the qualifications of the personnel being replaced. NRC reserves the right to deny Key Personnel designation for any individual, for any reason, at any time, during the life of this Contract.

It is a mandatory requirement for at least one of the key personnel to be certified as an ITIL v3 Expert. That ITIL v3 Expert certification of at least one Key Personnel must be maintained throughout the ITISS period of performance.

Prior to any Key Personnel reassignment, removal, or resignation, the offeror shall provide written notification. No replacement of key personnel shall be made by the offeror without the written consent of the CO.

Key Personnel shall be proposed in response to this contract request for the following positions:

C.8.1 Core Services

The following key personnel will be required to perform the Core Services (as described in section C.5 Core Services) under this contract:

1. Project Manager
2. Integration Manager/ITI Architect
3. Operations Manager
4. IT Security Operations & Compliance Manager
5. Configuration/Asset Manager
6. Transition and Quality Assurance Manager
7. Service Desk Manager

The offeror's ITISS Project Manager will be empowered to make decisions related to this contract independently without consulting the offeror's corporate management.

C.8.2 Optional Services

The following additional key personnel will be required to perform the specified optional tasks under this contract:

1. Data Center Operations Manager

   C.6.1 Computer Facilities Management

   C.6.3 Data Center System Administration
2. Incident Response Manager

   C.6.2 NSIR Operations Center Network Management

C.6.8 ERDS Operations and Maintenance

3. Software License Project Lead

   C.6.5 Software License Management

4. Document Management Lead

   C.6.9 ESafe Records and Document Management Services

C.9 WORKING ONSITE AT NRC FACILITIES

(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 System 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 offerors, contractors, sub-contractors, 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 sensitive unclassified information (Safeguards, Official Use Only, and Proprietary 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 offeror's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The offeror 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 offeror's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the offeror shall, upon completion or termination of this contract, transmit to the Commission and classified matter in the possession of the offeror or any person under the offeror's control in connection with performance of this contract. If retention by the offeror of any classified material is required after the completion or termination of the contract and the retention is approved by the contracting officer, the offeror 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 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 work under this contract, the offeror 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 offeror 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 offeror will not directly or indirectly duplicate, disseminate, or disclose the information in whole or part to any other person or organization except as may be necessary to perform the work under this contract. The offeror 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 offeror 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 offeror 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 offeror 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 offeror 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 offeror or any person under the offeror's control in connection with work under this contract, may subject the offeror, its agents, employees or sub-contractors 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 offeror shall insert provisions similar to the foregoing in all subcontracts and purchase orders under this contract.

(l) In performing the contract work, the offeror shall classify all documents, material and equipment originated or generated by the offeror 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 sub-contractor or supplier assign classification to all documents, material, and equipment in accordance with the guidelines furnished by the offeror.