ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 | 46

IMPORTANT: Mark all packages and papers with contract and/or order numbers. BPA NO.

1. DATE OF ORDER: 02-23-2010	2. CONTRACT NO. (If any): GS-35F-4507G
3. ORDER NO.: NRC-DR-21-10-495	MODIFICATION NO.:	4. REQUISITION/REFERENCE NO.:

5. ISSUING OFFICE (Address correspondence to)
U.S. Nuclear Regulatory Commission
Division of Contracts
Attn: Michael Turner
Mail Stop: TWB-01-B10M
Washington, DC 20555

6. SHIP TO:
a. NAME OF CONSIGNEE: U.S. Nuclear Regulatory Commission
b. STREET ADDRESS: Atomic Safety and Licensing Board Panel
Attn: Matt Schmit
Mail Stop: T-3-F23

c. CITY	d. STATE	e. ZIP CODE
Washington	DC	20555

7. TO:
a. NAME OF CONTRACTOR: AT&T GOVERNMENT SOLUTIONS, INC.
AT&T (DUNS: 009683442)
b. COMPANY NAME:
c. STREET ADDRESS: 1900 GALLOWS RD STE 105

d. CITY	e. STATE	f. ZIP CODE
VIENNA	VA	221823865

f. SHIP VIA:

8. TYPE OF ORDER
[ ] a. PURCHASE — REFERENCE YOUR _____ Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
[X] b. DELIVERY — Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
B&R#: 07D-15-300-189 Job Code#: M7027 BOC#: 252A
APPN#: 31N0200 FFS#: ASL10305 Obligation: $600,000.00

10. REQUISITIONING OFFICE: ASB

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
[ ] a. SMALL [X] b. OTHER THAN SMALL [ ] c. DISADVANTAGED [ ] g. SERVICE-DISABLED VETERAN-OWNED
[ ] d. WOMEN-OWNED [ ] e. HUBZone [ ] f. EMERGING SMALLBUSINESS

12. F.O.B. POINT:

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE		As stated	Net 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The Contractor shall provide the U.S. Nuclear Regulatory Commission with Operations and Maintenance Support for the Licensing Support Network (LSN) in accordance with AT&T GSA Federal Supply Schedule Contracts GS-35F-4507G and GS-35F-0249J, the enclosed Statement of Work, at the prices set forth in the Schedule of Supplies or Services and Prices/Costs. This order shall be effective February 25, 2010, through February 24, 2011 for the total estimated amount (ceiling) of $848,802.22. There are four one-year options as follows: Option Year 1 $891,392.92; Option Year 2 $934,025.22; Option Year 3 $1,013,307.12; and Option Year 4 $ $1,061,679.84. The total estimate amount (ceiling) of this order including options is $4,749,207.65. Reference is made to AT&T Government Solutions proposal dated October 2, 2009, as amended January 28, 2010 and and February 18, 2010, to extend the due for acceptance of your proposal in response to this effort.					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	$848,802.22	17(h) TOTAL (Cont. pages)

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:
a. NAME: Department of Interior / NBC
NRCPayments@nbc.gov
b. STREET ADDRESS (or P.O. Box): Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue

c. CITY	d. STATE	e. ZIP CODE	$4,749,207.65	17(i). GRAND TOTAL
Denver	CO	80235-2230		

22. UNITED STATES OF AMERICA
BY (Signature): Michael A. Turner

23. NAME (Typed)
Michael A. Turner,
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE MAY 26 2010

ADM002

Please indicate your acceptance of this order by having an official who is authorized to bind your organization, execute this document in the spaces provided below.

ACCEPTED:

April V. Pulliam
NAME

Contract Manager
TITLE

2/24/10
DATE

Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

A.2 2052.215-70 KEY PERSONNEL (JAN 1993)

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

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 con-currence 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.

A.3 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 therefor (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.

A.4 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.

A.5 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.

A.6 52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond February 24, 2011. 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 February 24, 2011, 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.

A.7 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 60 days; 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 5 years.

A.9 DURATION OF CONTRACT PERIOD (MAR 1987) ALTERNATE 4 (JUN 1988)

The ordering period for this contract shall commence on February 25, 2010, and will expire on February 24, 2011. The term of this contract may be extended at the option of the Government for an additional 4 year years.

A.9 OPTION PERIODS - TASK ORDER/DELIVERY ORDER UNDER A GSA FEDERAL SUPPLY SCHEDULE CONTRACT (MARCH 2007)

The Period of Performance (POP) for this requirement may extend beyond the Offeror's current POP on their GSA Schedule. Offerors may submit proposals for the entire PoP as long as their current GSA Schedule covers the requested PoP, or their GSA Schedule contains GSA's "Evergreen Clause" (Option to Extend the Term of the Contract), which covers the requested POP if/when the option(s) are exercised. Offerors are encouraged to submit accurate/realistic pricing for the requirement's entire POP, even if the proposed GSA Schedule does not include pricing for the applicable option years, etc.

For proposal evaluation purposes, the NRC assumes that applicable Evergreen Clause Option(s) will be exercised and the NRC will apply price analysis, as applicable. It is in the best interest of the Offeror to explain major deviations in escalation, proposed in any Evergreen Clause option years. Resulting GSA task/delivery order option years subject to the Evergreen Clause will be initially priced utilizing the same rates proposed under the last GSA-priced year of the subject GSA Schedule. Upon GSA's exercise of the GSA Schedule option year(s) applicable to the Evergreen Clause, the NRC will modify the awarded task/delivery order to incorporate either the proposed pricing for the option years or the GSA-approved pricing (whichever is lower).

It is incumbent upon the Offeror to provide sufficient documentation (GSA-signed schedule, schedule modifications, etc.) that shows both the effective dates, pricing and terms/conditions of the current GSA Schedule, as well as Evergreen Clause terms/conditions (as applicable). Failure to provide this documentation may result in the Offeror's proposal being found unacceptable.

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

BASE PERIOD – YEAR ONE

FIXED PRICE SERVICES

CLIN	Description	Quantity	Unit	Unit Price	Firm-Fixed Price
0001	Participant Integration - (Task 2)	[redacted]	Mos.	[redacted]	[redacted]
0002	Hardware/Software Installation and Maintenance (Hosting) - (Task 3)	[redacted]	Mos.	[redacted]	[redacted]
0003	Status Reporting - (Task 7)	[redacted]	Mos.	[redacted]	[redacted]
0004	Web Page Maintenance/Update - (Task 8)	[redacted]	Mos.	[redacted]	[redacted]
0005	Hardware Refresh - (Task 10)	[redacted]	Ea.	[redacted]	[redacted]
Subtotal					[redacted]

LABOR HOUR SERVICES

CLIN 0006 – Document Availability (Task 1)
CLIN 0007 – Test Environment (Task 4)
CLIN 0008 – System Security (Task 5)
CLIN 0009 – Release-Based and Emergency Maintenance Support (Task 6)
CLIN 0010 – Administration Subsystem Maintenance (Task 9)

Labor Category	Estimated Hours	Labor Rate	Total Estimated Costs
Principle SW Design Engineer	[redacted]	[redacted]	[redacted]
Systems Analyst/Programmer	[redacted]	[redacted]	[redacted]
Sr. Systems Analyst/Programmer	[redacted]	[redacted]	[redacted]
INFOSEC Specialist	[redacted]	[redacted]	[redacted]
Subtotal:			[redacted]

Total Estimated Amount – Base Year **$848,802.55**

OPTION YEAR ONE – YEAR TWO

FIXED PRICE SERVICES

CLIN	Description	Quantity	Unit	Unit Price	Firm-Fixed Price
0011	Participant Integration - (Task 2)	[redacted]	Mos.	[redacted]	[redacted]
0012	Hardware/Software Installation and Maintenance (Hosting) - (Task 3)	[redacted]	Mos.	[redacted]	[redacted]
0013	Status Reporting - (Task 7)	[redacted]	Mos.	[redacted]	[redacted]
0014	Web Page Maintenance/Update - (Task 8)	[redacted]	Mos.	[redacted]	[redacted]
0015	Hardware Refresh - (Task 10)	N/A	N/A	N/A	N/A
Subtotal					[redacted]

LABOR HOUR SERVICES			
CLIN 0016 - Document Availability (Task 1) **CLIN 0017** - Test Environment (Task 4) **CLIN 0018** - System Security (Task 5) **CLIN 0019** - Release-Based and Emergency Maintenance Support (Task 6) **CLIN 0020** - Administration Subsystem Maintenance (Task 9)			
Labor Category	**Estimated Hours**	**Labor Rate**	**Total Estimated Costs**
Principle SW Design Engineer	[redacted]	[redacted]	[redacted]
Systems Analyst/Programmer			
Sr. Systems Analyst/Programmer			
INFOSEC Specialist			
Subtotal:			[redacted]

Total Estimated Amount – Option Year One **$891,392.92**

OPTION YEAR TWO – YEAR THREE

FIXED PRICE SERVICES					
CLIN	**Description**	**Quantity**	**Unit**	**Unit Price**	**Firm-Fixed Price**
0021	Participant Integration - (Task 2)	[redacted]	Mos.	[redacted]	[redacted]
0022	Hardware/Software Installation and Maintenance (Hosting) - (Task 3)		Mos.		
0023	Status Reporting - (Task 7)	[redacted]	Mos.	[redacted]	[redacted]
0024	Web Page Maintenance/Update - (Task 8)		Mos.		
0025	Hardware Refresh - (Task 10)	N/A	N/A	N/A	N/A
Subtotal					[redacted]

LABOR HOUR SERVICES			
CLIN 0026 - Document Availability (Task 1) **CLIN 0027** - Test Environment (Task 4) **CLIN 0028** - System Security (Task 5) **CLIN 0029** - Release-Based and Emergency Maintenance Support (Task 6) **CLIN 0030** - Administration Subsystem Maintenance (Task 9)			
Labor Category	**Estimated Hours**	**Labor Rate**	**Total Estimated Costs**
Principle SW Design Engineer	[redacted]	[redacted]	[redacted]
Systems Analyst/Programmer			
Sr. Systems Analyst/Programmer			
INFOSEC Specialist			
Subtotal:			[redacted]

Total Estimated Amount – Option Year Two **$ 934,025.22**

OPTION YEAR THREE – YEAR FOUR

FIXED PRICE SERVICES					
CLIN	**Description**	**Quantity**	**Unit**	**Unit Price**	**Firm-Fixed Price**
0031	Participant Integration - (Task 2)	[redacted]	Mos.	[redacted]	[redacted]
0032	Hardware/Software Installation and Maintenance (Hosting) - (Task 3)	[redacted]	Mos.	[redacted]	[redacted]
0033	Status Reporting - (Task 7)	[redacted]	Mos.	[redacted]	[redacted]
0034	Web Page Maintenance/Update - (Task 8)	[redacted]	Mos.	[redacted]03	$ [redacted]
0035	Hardware Refresh - (Task 10)	N/A	N/A	N/A	N/A
Subtotal					[redacted]

LABOR HOUR SERVICES			
CLIN 0036 - Document Availability (Task 1) **CLIN 0037** - Test Environment (Task 4) **CLIN 0038** - System Security (Task 5) **CLIN 0039** - Release-Based and Emergency Maintenance Support (Task 6) **CLIN 0040** - Administration Subsystem Maintenance (Task 9)			
Labor Category	**Estimated Hours**	**Labor Rate**	**Total Estimated Costs**
Principle SW Design Engineer	[redacted]	[redacted]	[redacted]
Systems Analyst/Programmer	[redacted]	[redacted]	[redacted]
Sr. Systems Analyst/Programmer	[redacted]	[redacted]	[redacted]
INFOSEC Specialist	[redacted]	[redacted]	[redacted]
Subtotal:			[redacted]

Total Estimated Amount – Option Year Three **$1,013,307.12**

OPTION YEAR FOUR – YEAR FIVE

FIXED PRICE SERVICES					
CLIN	**Description**	**Quantity**	**Unit**	**Unit Price**	**Firm-Fixed Price**
0041	Participant Integration - (Task 2)	12	Mos.	$ 5,997.93	$ 71,975.16
0042	Hardware/Software Installation and Maintenance (Hosting) - (Task 3)	12	Mos.	$15,887.40	$190,648.80
0043	Status Reporting - (Task 7)	12	Mos.	$ 6,517.95	$ 78,215.40
0044	Web Page Maintenance/Update - (Task 8)	12	Mos.	$ 5,759.55	$ 69,114.60
0045	Hardware Refresh - (Task 10)	N/A	N/A	N/A	N/A
Subtotal					**$409,953.96**

LABOR HOUR SERVICES			
CLIN 0046 - Document Availability (Task 1) **CLIN 0047** - Test Environment (Task 4) **CLIN 0048** - System Security (Task 5) **CLIN 0049** - Release-Based and Emergency Maintenance Support (Task 6) **CLIN 0050** - Administration Subsystem Maintenance (Task 9)			
Labor Category	**Estimated Hours**	**Labor Rate**	**Total Estimated Costs**
Principle SW Design Engineer	[redacted]	[redacted]	[redacted]
Systems Analyst/Programmer			
Sr. Systems Analyst/Programmer			
INFOSEC Specialist			
Subtotal:			[redacted]

Total Estimated Amount – Option Year Four **$1,061,679.84**

Total Estimated Amount - Base and Option Years 1 – 4 **$4,749,207.65**

B.2 CONSIDERATION AND OBLIGATION

a. The total estimated amount (ceiling) for the products/services ordered, delivered, and accepted under this contract is **$848,802.55**. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this contract.

b. The amount presently obligated with respect to this contract is **$600,000.00**. The Contracting Officer may issue orders for work up to the amount presently obligated. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the ceiling as specified in paragraph a above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

OPERATIONS AND MAINTENANCE SUPPORT SERVICES FOR THE LICENSING SUPPORT NETWORK
Performance-Based Statement of Work (PBSOW)

C.1 BACKGROUND:

Section 114 (d) of the Nuclear Waste Policy Act of 1982 (NWPA) requires the Nuclear Regulatory Commission (NRC) to issue a final decision approving or disapproving issuance of the construction authorization for a mined geologic repository to store High-Level radioactive Waste (HLW) at Yucca Mountain, NV. The NRC expects to accomplish this by replacing the classic "discovery" exchanges among parties with internet-based electronic access to discovery materials, via the Licensing Support Network (LSN), at www.lsnnet.gov. The LSN, which is a critical tool for the HLW proceeding, is intended to ensure that document access, and the associated hearing agenda, can all be handled in an expeditious and efficient manner.

The LSN is codified in Title 10 of the Code of Federal Regulations (10 CFR) Part 2, Subpart J. Since the original rule was promulgated in 1989 seeking to establish a centralized dial-up Licensing Support System, there has been extensive technological innovation regarding the system, much of it the result of interaction with the parties and potential parties to the HLW proceeding under the auspices of a federal advisory committee, now known as the LSN, Advisory Review Panel (LSNARP), that was chartered to provide advice and guidance on the design and operation of the system. The LSN fosters the NRC's ability to protect public health and safety with respect to a licensing decision on the HLW repository by:

- facilitating the NRC's compliance with the mandated 3 to 4-year schedule for a decision on the repository construction authorization,
- providing an electronic environment that facilitates a thorough technical review of relevant HLW proceeding documentary material, and
- ensuring equitable access to the information for the parties to the hearing as well as members of the public.

The LSN provides a web-based portal (www.lsnnet.gov), or central index, to the HLW proceeding participants' documents. Users follow links to relevant materials from the LSN site or issue searches using fielded or text queries. However, when a user selects a document for retrieval from the search results list, the request is delivered by the LSN (through a HTTP link) to the participant's machine where the participant documents are located. The 19 current LSN participants are DOE (two sites), NRC, the State of Nevada, the Nevada counties of Nye, White Pine, Mineral, Churchill, Clark, Eureka, Lander, Lincoln, and Esmeralda, the Nuclear Energy Institute (NEI), the City of Las Vegas, Nevada, Inyo County, California, the California Energy Commission, Timbisha Shoshone Tribe, Timbisha Shoshone Yucca Oversight Program, and the City of Caliente, Nevada, for a total of 20 websites that have been integrated. Although no additional participants are expected, the possibility exists for one or two additional participants to be added.

The LSN indexing subsystem is a set of software routines that provides the ability to process (e.g., index) 20,000 pages per day for loading into the LSN search subsystem. Currently the LSN search subsystem contains approximately 3.6 million documents (36 million pages). The maximum system capacity is 5 million documents (50 million pages).[1] Currently, 20 participant web sites are integrated and regularly spidered by the LSN. In addition, the LSN administration subsystem allows the LSN project team to monitor the LSN (e.g., identify new or changed documents) and update web site information (e.g., post announcements and add priority users).

The overall operating environment includes but is not limited to:

- Microsoft (MS) SQL Server 2003.
- Windows server leveraging load balancing and clustering.
- Overland storage tape subsystem.
- Autonomy IDOL (Intelligent Data Operating Layer) Server (12 IDOL Severs), Distributed Index Handler (DIH), and Distributed Action Handler (DAH).
- Secure FTP (File Transfer Protocol).
- Web Server (Internet Information Server 6).
- XML (Extensible Markup Language).
- Storage Area Network (SAN).
- MS Visual Studio (.Net and Visual Basic).

C.2 OBJECTIVES

The objective of the LSN is to ensure that document access, and the associated hearing agenda, can all be handled in an expeditious and efficient manner thereby reducing the time needed to conduct the HLW repository licensing proceeding. The contractor shall provide the necessary hardware and software maintenance, labor, web application hosting, and other resources needed to ensure uninterrupted operation of the LSN throughout the Yucca Mountain HLW repository licensing proceeding.

---

1 Current LSN capacity is approximately 5 million documents and 50 million pages. System capacity is not expected to be exceeded during the course of this contract period of performance. However, should system reengineering to resize the capacity be necessary, it is considered part of routine maintenance and is included in Task 6. Note that the hardware and software required for such resizing is separately provided to the operations and maintenance contractor as Government Furnished Equipment (GFE) and therefore is not included in the scope of this contract.

C.3 SCOPE OF WORK

The contractor shall maintain and operate the LSN search subsystem, indexing subsystem, and administration subsystem. The scope of this project encompasses the following activities.

- Making documents submitted by participants available for search and retrieval via the LSN System.
- Maintaining the 19 currently integrated participants and integrate new participants (estimated at 2) for a total of approximately 21.
- Providing a secure co-hosting facility with a minimum 3Mbps (megabits per second) bandwidth, firewall, and Intrusion Detection System (IDS).
- Maintaining a test environment at the contractor's facility.
- Assisting the LSN project team in meeting Federal Information Security Management Act (FISMA) requirements, including recertification and accreditation of the LSN.
- Providing routine maintenance.
- Providing status reporting.
- Maintaining and updating Web pages.
- Maintaining the LSN administration subsystem.
- Hardware "refresh."

The contractor shall address and comply with all NIST 800-53 requirements consistent with low baseline security controls and additional controls as deemed necessary by the sensitivity of information being processed and the nature of the system.

C.4 CONTRACT TASK

Task 1 – Document Availability

Requirement: The contractor shall make current documents submitted by participants available for search and retrieval via the LSN. Currently the LSN search subsystem contains approximately 3.6 million documents (36 million pages) that have been uploaded to the LSN search subsystem and are available to the HLW proceeding parties and the public for search and retrieval. The current system capacity is 5 million documents (50 million pages). The contractor shall upload the documents and make them available for search and retrieval 24 hours a day, 7 days a week, and 365 days a year. The LSN spider (document upload process) is a set of software routines that provide the ability to process (e.g., index) documents

for loading into the search subsystem. The contractor shall process/upload (via the spidering process) new, deleted, and changed documents made available by participants within 24 hours of receipt (or as directed by the LSN project team). The contractor shall process daily, when made available by a participant, a maximum document load of 20,000 documents (approximately 200,000 pages) per night, 5 nights per week, for a total of 100,000 documents (approximately 1 million pages) per week. Participant materials are prepared and made available for indexing in accordance with LSN Administrator guidelines (see Attachment 2, Setting Up an LSN Repository, which provides guidance for participants on how to make their site available for integration into the LSN).

Maximum downtime (e.g., cannot search and retrieve documents due to a system error) shall be less then 4 hours Monday-Friday (excluding holidays) during working hours (6:00 a.m. Eastern Time (ET) - 9:00 p.m. ET) per day. After working hours, on weekends, and on holidays, the maximum downtime shall be 8 hours per day. The LSN project team shall be given a minimum of 24 hours notice of any contractor-planned maintenance that may affect LSN operations.

The LSN shall accept documents made available in standard text formats including, but not limited to, Word, WordPerfect, Portable Document Format, Hypertext Markup Language, text file, and PowerPoint. Additionally, documents with no text (e.g., image-only documents or header only documents with no image) must also be made available for bibliographic header field-only search and retrieval. Image formats include, but are not limited to, single-page Tag Image File Format (TIFF), multi-page TIFF, Graphics Interchange Format (GIF), and Joint Photographic Experts Group. Bibliographic header field information will be posted in XML format by LSN participants.

Performance Standards: The contractor shall ensure that 100 percent of the documents posted by participants are uploaded (i.e., successfully spidered) within 24 hours or as directed by the LSN Project team. If a participant's document(s) cannot be successfully spidered (e.g., corrupt document file, invalid XML header file, etc.), this shall be reported in the LSN administration subsystem. Documents successfully spidered shall be available for search and retrieval by users 24 hours a day, 7 days a week, and 365 days a year. The maximum unavailability of the LSN search system shall be less then 4 hours during the hours of 6:00 a.m. ET and 9:00 p.m. ET and less then 8 hours at any other time.

Deliverable: The data from the spider shall be immediately uploaded to the LSN administration system within one hour of each spider run.

Method of Surveillance: The LSN has an administration subsystem that identifies the number of documents successfully spidered. If a document is not successfully spidered, it shall be reported in the LSN administration subsystem. The LSN project officer will use this administrative module on a daily basis to verify successful and/or unsuccessful document uploads. If a document is not successfully uploaded, the contractor shall work with the LSN project team to identify what caused the error in effort to allow the participant to remedy document upload anomalies (e.g., corrupt document file, invalid header XML file, etc.). Additionally, the LSN project team will independently verify the search system is available by issuing queries and/or monitoring the LSN Webmaster E-mail account where users identify system problems.

Guidance: Attachment 1, Table A, Recommended Participant Bibliographic Header Field Structure, provides a description of the fields that shall be available for searching in the LSN.

Attachment 2, Setting Up an LSN Repository.

Acceptance:

1. One event per month causing either:

    - downtime of less then four hours Monday-Friday (excluding holidays) during working hours (6:00 a.m. ET - 9:00 p.m. ET) per day or

    - downtime of less then eight hours after working hours, on weekends, or on holidays.

2. Complete participant spidering at a maximum of 20,000 documents within 24 hours.

Task 2 – Participant Integration

Requirement: The contractor shall maintain the 19 currently integrated participants and integrate new participants (estimated at two) for a total of 21. Integration is completed with the LSN is able successfully to spider a participant document repository (see Task 1).

Performance Standard: New participants shall be integrated into the LSN System within two weeks of receiving the appropriate application/paperwork. Problems with previously integrated participants shall be diagnosed by the contractor within 24 hours. LSN problems identified by the contractor preventing participant integration shall be resolved by the contractor within 48 hours. The contractor shall work as expeditiously as possible to resolve integration problems caused by the participant (e.g., participant machine unavailability).

Deliverable: The new participant is posted on the LSN advanced search page when integration is completed.

Method of Surveillance: The LSN has an administration subsystem that identifies the number of current participants. The LSN project officer will use this administrative module to determine whether new participants have been added within two weeks of receiving an application. The administrative subsystem will also be used to identify whether previously integrated participants are still active by reviewing the spider reports (e.g., successful document uploads, changes, and/or deletes).

Guidance: Attachment 2, Setting Up an LSN Repository, provides guidance for participants on how to make their site available for integration into the LSN. The contractor can use this guidance document to gain an understanding of how participant sites are to be configured for integration with the LSN.

Acceptance:

1. New participant is integrated within two weeks of receiving request.

2. One participant integration problem caused by the LSN in every five is solved by the contractor in 48-72 hours.

Task 3 – Hardware/Software Installation and Maintenance – (Hosting)

Requirement: The contractor shall install and maintain the LSN hardware and software in a secure co-hosting facility with a minimum 3Mbps (Megabits per second) bandwidth Internet connection, firewall, and Intrusion Detection System (IDS). Attachment 3, LSN Network Diagram, provides the current configuration of the system. Any changes to the configuration must be approved by the LSN project team. A breach of the LSN by a hacker shall be prevented. The LSN shall be protected against viruses. Other malicious activity, such as denial of service attacks, shall be minimized to the maximum extent possible.

The contractor shall provide application installation and maintenance support, as necessary and as directed by the LSN Project Officer, to address requirements identified in the LSN Plan of Action and Milestones (POA&M).

Performance Standard: No breach to the LSN by unauthorized users (e.g. hackers). Minimum 3Mbps bandwidth. Denial of service attack (or other malicious activity) response by the contractor shall ensure that LSN search and retrieval unavailability is limited to no more than 4 consecutive hours in any one day Monday-Friday (excluding holidays) during working hours (6:00 a.m. ET -9:00 p.m. ET). After working hours, on weekends, and on holidays, the maximum LSN search and retrieval downtime shall be eight hours per day.

POA&M action items are delivered on or before agreed-upon schedule.

Deliverable: With the monthly report (see Task 7) a report of firewall and IDS activity including any recommended adjustments to bolster LSN security (e.g., changes in firewall or IDS rule sets to prevent potential hacker attacks).

Method of Surveillance: The LSN project team shall be placed on the IDS alert E-mail list.

Delivery of POA&M action items are reported in the monthly report.

Guidance: See Attachment 3, LSN Network Diagram, for the current configuration of the system.

Acceptance:

- Firewall and IDS activity report delivered no later then two days after the monthly report in one instance per year.

Task 4 – Test Environment

Requirement: The contractor shall maintain a test environment at the contractor's facility. The LSN test environment shall facilitate efficient development of LSN fixes and enhancements and shall be synchronized with the versions and releases utilized in the production system.

Performance Standard: Within 12 weeks of contract award the test environment shall be fully operational.

Deliverable: Maintain a fully operational test environment.

Method of Surveillance: Site visit within 14 weeks of contract award, and periodic visits thereafter.

Guidance: See Attachment 4, LSN Test Network Diagram.

Acceptance: Test environment operational within 12 weeks of contract award.

Task 5 – System Security

Requirement: The contractor shall assist the LSN project team in meeting Federal Information Security Management Act (FISMA) requirements. An Authority to Operate (ATO) was granted to the LSN in September 2007. The ATO is valid for 3 years. To maintain this ATO, the contractor shall complete annual requirements including creating a contingency plan test and report and a security self-assessment, and reviewing and updating a system security plan, an operations guide, and a risk assessment.

The contractor will assist the LSN project team in achieving recertification of the system prior to the expiration of the current ATO in September 2010. The LSN is a publicly available system that contains no classified materials, Safeguards Information, or text or images of sensitive, unclassified materials. Accordingly, its security categorization is low (on the risk scale of low, medium, and high).

The contractor shall provide support, as necessary and as directed by the LSN Project Officer, to address security requirements identified in the LSN Plan of Action and Milestones (POA&M).

Performance Standard: Complete the annual ATO deliverables by the dates specified by the LSN project officer. Lead time will be coordinated with the LSN project officer for each deliverable except the ATO, which must be completed prior to expiration of the existing system ATO in September 2010.

POA&M action items are delivered on or before agreed-upon schedule.

Deliverable:

Base Year: TBD – Update Contingency Plan
6/1 – Conduct and Document Contingency Plan Test

6/1 - Update System Security Plan
7/1 - Conduct and Document Security Self-Assessment
9/1 - Update Operations Guide

Option Year 1: Date TBD – Review and Update System Documentation in Preparation for Recertification Activities
3/1 – Update Contingency Plan
6/1 – Conduct and Document Contingency Plan Test
6/1 - Update System Security Plan
7/1 - Conduct and Document Security Self-Assessment
9/1 - Update Operations Guide
9/30/10 – Complete ATO

Option Year 2: 3/1 – Update Contingency Plan
6/1 – Conduct and Document Contingency Plan Test
6/1 - Update System Security Plan
7/1 - Conduct and Document Security Self-Assessment
9/1 - Update Operations Guide

Option Year 3: 3/1 – Update Contingency Plan
6/1 – Conduct and Document Contingency Plan Test
6/1 - Update System Security Plan
7/1 - Conduct and Document Security Self-Assessment
9/1 - Update Operations Guide

Option Year 4: 3/1 – Update Contingency Plan
6/1 – Conduct and Document Contingency Plan Test
6/1 - Update System Security Plan
7/1 - Conduct and Document Security Self-Assessment
9/1 - Update Operations Guide

Method of Surveillance: The LSN Project Officer shall evaluate the timeliness and completeness of all deliverables and POA&M action items.

Acceptance: Each deliverable shall be provided the date specified. Except for the ATO, delivery may be up to 1 month later than scheduled, with prior approval from the LSN project team, insofar as that delivery does not affect receiving the ATO on schedule. The contractor's requests for a change in the delivery date for any deliverable shall be submitted to the project officer no later then 30 days before the scheduled due date for that deliverable.

Task 6 – Release-Based and Emergency Maintenance Support

Requirement: The contractor shall provide general (release-based and emergency) maintenance support of the LSN application software, files, and databases, and all associated backup and recovery subsystems.

The contractor shall provide operational support for the LSN search and administrative subsystems, and for all associated backup and recovery subsystems, including scheduled

reviews subsequent to participant sites being "spidered" and the LSN indexes being updated. The contractor shall monitor the LSN every business day, to ensure correct, stable, and efficient operation of the system, including, but not limited to (1) verifying system operation; (2) checking the status of transaction and index updates resulting from scheduled "spidering" of participant sites; and (3) reviewing, on a daily basis, the operational reports and logs. On a scheduled basis (at least monthly), the contractor shall check the size, growth, space utilization, and integrity of the underlying RDBMS tables, control-point directories, and database structures, and perform other diagnostic routines to ensure successful LSN operation. The contractor shall administer user IDs and user access levels per requirements established in the overall design concept. The contractor shall respond to questions from the database administrators for the participants that provide document collections for LSN spidering regarding issues about keeping their LSN collections current, as directed by the LSN project manager.

When LSN maintenance and operational support responsibilities result in the discovery of an actual or potential LSN problem that needs to be further diagnosed and/or corrected, or when database monitoring identifies a database change that is needed, the contractor shall promptly notify the LSN Project Officer via phone and/or e-mail. The contractor shall provide resources to perform an ad hoc analysis of the LSN application code, scripts, agents, and database tables in response to technical questions from the LSN Project Officer.

The contractor shall make routine and ad hoc preventive and corrective changes to the LSN databases as requested or approved by the LSN project manager. In general, these changes shall either be to crawlers, scripts, agents, the database structures, and/or the data definitions, or shall be for the purpose of correcting data in the databases. Additionally, the contractor should anticipate routine and corrective maintenance activities such as resizing the database, performing diagnostics on data in the database, running maintenance and backup jobs, etc.

During the duration of this contract it may be necessary to upgrade core software components such as Autonomy, SQL Server, .Net, etc. The upgrades may be necessary to fix an existing problem, prevent future problems, or maintain software currency for which there is third party support (e.g., Autonomy, BakBone). The LSN Project Officer must be notified during the planning stage of any proposed upgrades. In addition, upgrades must be fully tested on the test environment before they are implemented on the production system.

The contractor shall provide applications support, as necessary and as directed by the LSN Project Officer, to address requirements identified in the LSN Plan of Action and Milestones (POA&M).

Performance Standard: Maximum downtime, (e.g., cannot search and retrieve documents due to maintenance issue) shall be less than 4 hours Monday-Friday (excluding holidays) during working hours (6:00 a.m. ET - 9:00 p.m. ET) per day. After working hours, on weekends, and on holidays, the maximum downtime shall be 8 hours per day.

POA&M action items are delivered on or before agreed-upon schedule.

Deliverable: Planned maintenance activities shall be coordinated with the LSN Project Officer via telephone or E-mail. Planned and completed maintenance activities and POA&M action item deliverables shall be noted in the weekly and monthly reports (see Task 7).

Method of Surveillance: The LSN administration subsystem will be used to review server performance, disk space utilization, and spider performance (e.g., documents successfully added). Additionally, the LSN project team will independently verify the search system is available by issuing queries and/or monitoring the LSN Webmaster e-mail account that is utilized by LSN users to identify system problems.

Acceptance: One event per month causing either:

1. downtime of less then 4 hours Monday-Friday (excluding holidays) during working hours (6:00 a.m. ET - 9:00 p.m. ET) per day or

2. downtime of less than 8 hours after working hours, on weekends, or on holidays.

Task 7 – Status Reporting

Requirement: Provide status reporting. The contractor shall provide weekly activity reports, which will include a discussion of any exceptions to or changes from the existing project plans. The weekly report will be delivered by Tuesday Close of Business (COB). The weekly will include a proposed agenda for discussing management issues and any technical issues that would impact schedule, cost, or operations. At a minimum, the weekly report should cover accomplished items, planned items, outstanding issues (technical, management, and financial), and proposed issue resolutions during the reporting period. No weekly meeting with the LSN project team is necessary unless there are significant issues to discuss. However, the weekly report must be delivered to the LSN project team via e-mail even though there is no meeting.

The monthly report shall include a narrative discussing items accomplished during the current reporting period, planned items for the next reporting period, identified technical, management or contractual issues, financial data (planned and actual) for the past month and for project-to-date, and an update to the project plan (in MS Project). The contractor must be able to establish an interface with NRC's IBM Rational Software Suite for integrated defect tracking, functional testing, and quality monitoring, as needed. The contractor shall meet monthly with the LSN project team to present the monthly report.

Performance Standard: Weekly Activity Report received by COB each Tuesday and Monthly Progress Reports received within 15 days after the end of a reporting period.

Deliverable: Weekly Activity Report and Monthly Progress Report

Method of Surveillance: The LSN Project Officer shall review weekly/monthly reports for accuracy, completeness, and timeliness.

Acceptance: Reports received by the specified dates.

Task 8 – Web Page Maintenance/Update

Requirement: The contractor shall maintain and update Web pages. Any web page updates or corrections shall be made by the contractor within 24 hours of notification from the LSN project team. If the changes require greater than 24 hours from notification, within 24 hours from notification the contractor shall deliver a web page update plan to the LSN project team that identifies the activities to be performed with associated completion dates. Any additional information or resources from the government (e.g., Government-Furnished Information (GFI) or Government-Furnished Equipment (GFE)) required by the contractor to complete the web page update shall be included in the plan. A maximum of two web page updates per month are estimated.

Performance Standard: Any web page updates or corrections shall be made by the contractor within 24 hours of notification from the LSN project team. If the changes require greater than 24 hours from notification, the contractor shall deliver a web page update plan to the government within 24 hours of notification.

Deliverable: Web page update plan

Method of Surveillance: The LSN project team will review the web site changes/updates or the web page update plan for accuracy, completeness, and timeliness.

Acceptance: One web page update per month taking more than 72 hours from notification that is not included in a timely web page update plan.

Task 9 – Administration Subsystem Maintenance

Requirement: The contractor shall maintain the LSN administration subsystem. The administration subsystem is used by the LSN project team to maintain the LSN as well as "audit" activity on the site. The administrative subsystem's functionality includes:

- Monitoring spider status, including progress within each stage (i.e., initialization, header fetch, header parse, document fetch, document index, document import, and successful transfer). Errors in any spidering stage are captured.
- Viewing repository status for each participant's document collection, which includes the number of headers, documents, and document sections indexed.
- Auditing status, which provides random auditing of participant documents for changes. The changes are determined by a review of document file time, date, and/or MD5 changes. The LSN project team also has the ability to submit documents for auditing.
- Participant sever polling, which allows the LSN project team to determine if a participant's site (web or fetch server) is or has been down for a period of time (e.g., greater then 5 minutes).
- Viewing users on the web site by internet protocol (IP) or login name.

- Providing LSN server status for each system machine, including central processing unit (CPU) and memory utilization.

- Generating date-based reports for each participant that reports processing errors (e.g., fetch errors, parse errors), new documents, modified headers, modified documents, and/or deleted documents.

- Adding a new participant to the system and setting its site accessibility to active, visible but not searchable, or not visible.

- Adding priority users.

- Managing data, such as adding announcements, guidance, help pages, events, hyperlinks, frequently asked questions (FAQs), tutorials, downloads, and home page notices.

- Setting the query mode to all queries, no public queries, and priority queries, so as to provide control over who is permitted to log in based on query server CPU utilization thresholds.

The contractor shall keep an updated defect log. The existing defect log, maintained in MS Excel, shall be provided to the contractor by the LSN project team within one week of contract award.

The contractor shall provide administration subsystem maintenance and application support, as necessary and as directed by the LSN Project Officer, to address requirements identified in the LSN Plan of Action and Milestones (POA&M).

Performance Standard: Any defect identified by the LSN project team shall be fixed in one week. POA&M action items are delivered on or before agreed-upon schedule.

Deliverable: Updated defects log with the monthly report or within 24 hours when new items are added.

Method of Surveillance: The LSN project team will review the defect log for accuracy, completeness, and timeliness. POA&M action items are reported in the weekly and monthly reports, and are reviewed and evaluated by the Project Officer.

Acceptance: One defect per month fixed by the contractor within 2 weeks of the time the contractor is notified of the defect by the LSN project team.

Task 10 – Hardware Refresh

Requirement: The contractor shall provide the services necessary to "refresh" all the LSN hardware with new replacement hardware. The hardware will be acquired by the LSN project team and provided to the contractor as GFE. The contractor shall coordinate with the LSN project team to ensure architecturally-compatible replacement machines are identified and acquired by developing a Hardware Upgrade Specification. The contractor shall be responsible for taking delivery of and installing the hardware. Although the refresh will focus on production

equipment, some of the equipment in the test lab also may be replaced. The contractor shall conduct an analysis of which, if any, test lab equipment should be replaced and include a list of that equipment in the Hardware Upgrade Specification. The test lab configuration and equipment should reflect, as much as practical, the production environment to allow for accurate and efficient testing of upgrades and fixes.

The contractor shall provide support, as necessary and as directed by the LSN Project Officer, to address requirements associated with equipment refresh efforts as identified in the LSN Plan of Action and Milestones (POA&M).

Performance Standard: Once approved by the LSN project team, the contractor shall take delivery of and install the equipment as specified in the Hardware Upgrade Plan. POA&M action items are delivered as part of the approved hardware upgrade.

Deliverable: January 2010 – Hardware Upgrade Specification
February 2010 – Hardware Upgrade Plan

Method of Surveillance: The LSN project team will review and approve the Hardware Upgrade Specification and the Hardware Upgrade Plan. Progress on the upgrade shall be reported in the weekly/monthly reports (see Task 7).

Guidance: Attachment 3, LSN Network Diagram
Attachment 4, LSN Test Network Diagram

Acceptance: Upgrade completed by the estimated completion date specified in the Hardware Update Plan.

C.5 MEETINGS AND TRAVEL

The contractor will be required to participate in weekly and monthly meetings to discuss the status reports. Meetings will be held at 10:00 a.m. ET on Wednesdays.

Minimal local travel will be required. One trip to Las Vegas, Nevada, for two contractor personnel may be required. For planning purposes, that trip will be one work week (5 working days) in length.

C.6 NRC-FURNISHED MATERIAL AND EQUIPMENT

All production and test system hardware, software, and operational documentation for the current LSN system will be provided by the LSN project team.

The contractor will provide the hardware and software necessary to connect to the Internet (e.g., hub, switch, router, firewall, IDS, etc.).

C.7 QUALITY ASSURANCE SURVEILLANCE PLAN

The Quality Assurance Surveillance Plan is designed to define the roles and responsibilities, identify the performance objectives, define the methodologies used to monitor and evaluate the contractor's performance, describe quality assurance reporting, and describe the analysis of quality assurance monitoring results.

The contractor's Quality Control Plan will set forth the staffing and procedures for self inspecting the performance requirements in the Statement of Work. The contractor will develop and implement a performance management system with processes to assess and report their performance to the project officer. The contractor shall bring problems affecting performance to the attention of the project officer and Contracting Officer as soon as possible.

The project officer will monitor performance and review performance to determine how the contractor is performing against communicated performance objectives. The project officer will make decisions based on performance measures and notify the contractor of those decisions. The contractor will be responsible for making required changes in process and practices to ensure performance is managed effectively.

The primary methods of surveillance are weekly/monthly checks, observations, and review of documents that are required to be maintained and delivered under this Statement of Work.

The Government's Quality Assurance (QA) monitoring, accomplished by the project officer, will be reported using the monitoring form in Section 9. The form, when completed, will document the project officer's understanding of the contractor's performance under the contract to ensure that the performance measures are being met. The project officer will retain a copy of all completed QA monitoring forms.

The project officer must coordinate and communicate with the contractor to resolve issues and concerns of marginal or unacceptable performance. The contractor shall adjust service accordingly to bring performance up to an acceptable level.

The project officer will notify the contractor of failure to meet standards through QA monitoring forms, cure notices, or show cause notices.

C.8 PERFORMANCE MEASURES

The contractor's performance will be evaluated using the performance metrics identified below:

Task One – Document Availability

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Availability for Search and retrieval.	Search and retrieval availability for users 24 hours a day, 7 days a week, 365 days a year. System non-availability less than 4 hours between 0600-2100 hours ET Monday through Friday (excluding government holidays).	Downtime of less then 4 hours Monday-Friday (excluding holidays) during working hours (6:00 a.m. ET-9:00 p.m. ET) per day, or downtime of less then 8 hours after working hours, on weekends, or on holidays	LSN Project Officer evaluation; LSN Webmaster e-mail traffic monitoring.	Quarterly incentive of $1,000 for search and retrieval availability for users 24 hours a day, 7 days a week, 365 days a year. $500 deduction from Contractor's invoice for system non-availability greater than 4 hours between 0600-2100 hours ET Monday through Friday (excluding government holidays).

Task Three – Hardware/Software Installation and Maintenance

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Install and maintain LSN hardware and software in secure co-hosting facility with minimum 3 Mbps bandwidth internet connection, firewall and Intrusion Detection System (IDS). Protect system against viruses, denial of service attacks, and other malicious activity. POA&M action items are addressed.	No breach of LSN by unauthorized users. Immediate Project Officer notification of critical firewall and IDS activity. No unauthorized configuration changes. No successful virus attacks. Immediate action to identify and counter denial of service attacks. POA&M items delivered on or before agreed upon schedule.	Firewall and IDS activity report delivered no later then two day after the monthly report.	Monthly report of critical firewall and IDS activity. IDS alert e-mail to LSN Project Officer. LSN Project Officer evaluation.	$5,000 annual incentive fee for no security events that impact the LSN operation. $5,000 annual deduction from the contractor's invoice for any security events that impact the LSN operation.

Task Five – System Security

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Support meeting FISMA requirements for Authority to Operate (ATO). POA&M action items are addressed.	Assist the LSN project team to attain the ATO prior to September 2010. POA&M items delivered on or before agreed upon schedule.	Delivered by agreed upon date	LSN Project Officer evaluation.	$2,500 incentive for LSN attaining the ATO during re-certification in September 2010.
Annual contingency plan test and report.	Complete per SOW requirements by date specified	Delivered received by agreed upon date	LSN Project Officer evaluation.	For each day reports are delivered late, beyond 14 days of the delivery date, $150 per day will be deducted from the contractor's invoice.
Security self assessment.	Complete per SOW requirements by date specified	Delivered by agreed upon date	LSN Project Officer evaluation.	For each day the assessment is delivered late, beyond 14 days of the delivery date, $150 per day will be deducted from the contractor's invoice.
Review and update SSP, Operations Guide, and Risk Assessment.	Complete per SOW requirements by date specified.	Delivered by agreed upon date	LSN Project Officer evaluation.	For each day the deliverables are delivered late, beyond 14 days of the delivery date, $150 per day will be deducted from the contractor's invoice.

Task Seven – Status Reporting

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Weekly activity report.	Deliver weekly/monthly report via E-mail by COB each Tuesday.	COB each Tuesday	LSN Project Officer evaluation.	For each day weekly/monthly reports are delivered late, beyond one day of the delivery date, $150 per day will be deducted from the contractor's invoice.

Task Eight – Web Page Maintenance/Update

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Maintain and update web pages.	Web page updates or corrections	Updates completed within 24-hour notification	LSN Project Officer evaluation.	For each day updates are posted late, beyond 72 hours of request by the Project Officer, $150 per day will be deducted from the contractor's invoice.

Task Ten – Hardware Refresh

Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Refresh production and test lab hardware with GFE equipment.	Complete per SOW requirements by date specified.	Completed by agreed upon date	LSN Project Officer evaluation.	For each day the refresh is completed late, beyond 7 days of the delivery date, $150 per day will be deducted from the contractor's invoice.
Hardware upgrade specification.	Complete per SOW requirements by date specified.	Delivered by agreed upon date	LSN Project Officer evaluation.	For each day the specification is delivered late, beyond 14 days of the delivery date, $150 per day will be deducted from the contractor's invoice.
Hardware upgrade plan. POA&M action items are addressed.	Complete per SOW requirements by date specified. POA&M items delivered on or before agreed upon schedule.	Delivered by agreed upon date	LSN Project Officer evaluation.	For each day the plan is delivered late, beyond 14 days of the delivery date, $150 per day will be deducted from the contractor's invoice.

C.9 QUALITY ASSURANCE SURVEILLANCE PLAN

This Quality Assurance Surveillance Plan (QASP) has been developed pursuant to the requirements of FAR 37.604. This plan sets forth procedures that will be used in evaluating the technical performance of the contractor.

A. Purpose of the QASP

1. The QASP is intended to accomplish the following:

a. Define the roles and responsibilities of participating government officials;
b. Define the types of work to be performed;
c. Describe the evaluation methods that will be employed by the government in assessing the contractor's performance;
d. Provide copies of the quality assurance monitoring forms that will be used by the government in documenting and evaluating the contractor's performance; and
e. Describe the process of performance documentation.

2. The contractor has developed a Quality Control Plan (QCP) which sets forth procedures and responsibilities for controlling high quality work. The contractor will designate an employee to be responsible for implementation of the QCP.

B. Roles and Responsibilities of Government Officials

The following government officials will participate in assessing the quality of the contractor's performance. Their roles and responsibilities are described as follows:

1. NRC Project Officer will be responsible for monitoring, assessing, recording and reporting on the technical performance of the contractor in accordance with the "Performance Requirement Summary". The PO will have primary responsibility for completing "Surveillance Monitoring Forms" which will be used to document the inspection and evaluation of the contractor's work performance.

2. The NRC Contract Specialist (CS) has overall responsibility for overseeing the contractor's performance. The CS will also be responsible for the day-to-day monitoring of the contractor's performance in the area of contract compliance and contract administration; reviewing the PO's assessment of the contractor's performance; and resolving all differences between the PO's version and the contractor's version.

C. Types of Work Performed

a. Operation and Maintenance Support Services

The contractor shall perform the following tasks as outlined in the Statement of Work:

Task 1 - Document Availability

Task 2 - Participant Integration

Task 3 - Hardware/Software Installation and Maintenance (Hosting)

Task 4 - Environment Testing

Task 5 - System Security

Task 6 - Released-Based and Emergency Maintenance Support

Task 7 - Status Reporting

Task 8 - Webpage Maintenance/Update

Task 9 - Administration Subsystem Maintenance

Task 10 - Hardware Refresh

3. D. Methods of Surveillance

The primary methods of surveillance for the above tasks are weekly/monthly checks, observations, and review of documents that are required to be maintained and delivered under this Statement of Work.

E. Quality Assurance Forms and Report

1. The PO will use the Surveillance Monitoring Form to document and evaluate the contractor's performance under the contract.

2. The PO will judge each requirement in accordance with the performance standards for each task.

3. The PO will substantiate all requirements which the PO judges to be indicative of "unacceptable" performance. Performance at the "acceptable" level is expected from the contractor and need not be substantiated.

4. The PO will forward copies of all completed surveillance monitoring forms to the CO and contractor upon completion of form. The contractor is required to respond in writing to any negative QA monitoring form(s) within 5 working days after receipt of the form.

F. Analysis of Surveillance Results

The CO will review each monitoring form prepared by the PO. When appropriate, the CO may investigate the performance event further to determine if all the facts and circumstances surrounding the event were considered in the PO's opinions outlined on the forms. The CO will discuss every event receiving a substandard rating with the contractor prior to the reduction in price.

G. Surveillance Monitoring Form

CONTRACT REQUIREMENT	CONTRACT SECTION	METHOD OF SURVEILLANCE	DATE PERFORMED	COMPLIANCE
Task One – Document Availability	Section C			
Task Two – Participant Integration	Section C			
Task Three – Hardware/Software Installation and Maintenance – (Hosting)	Section C			
Task Four – Test Environment	Section C			
Task Five – System Security	Section C			
Task Six – Released-Based and Emergency Maintenance Support	Section C			
Task Seven – Status Reporting	Section C			
Task Eight – Web Page Maintenance/Upgrade	Section C			
Task Nine – Administration Subsystem	Section C			
Task Ten – Hardware Refresh	Section C			

C.10 SECURITY CLAUSES

1. 2052.204-70 SECURITY (MARCH 2004)

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

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the Contracting Officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the Contracting Officer, the security provisions of the contract continue to be applicable to the matter retained.

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

The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the Contracting Officer. Failure to comply with this clause is grounds for termination of this contract.

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

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

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

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

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

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

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

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

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

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

2. BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MARCH 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 come into contact with.

3. 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 will pre-screen its applicants for the following:

(a) felony arrest in the last seven years; (b) alcohol related arrest within the last 5 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 7 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 within10 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 10 years.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 85P (Questionnaire for Public Trust Positions), 2 copies of the contractor's signed pre-screening record and two FD 258 fingerprint charts, through the Project Officer 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 10 years.

The contractor shall submit a completed security forms packet, including the OPM 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 Project Officer 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 Project Officer 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 Project Officer 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.

4. NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUGUST 2003)

NRC contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's 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 term of the contract within 3 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.

5. 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 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.

6. COMPUTER SECURITY REQUIREMENTS

- The contractor shall adhere to NRC policies, including but not limited to:
  - Management Directive 12.5, Automated Information Security Program,
  - Computer Security Incident Response Policy.

- 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.
- To the extent required to carry out a program of inspection to protect against threats and hazards to the security, availability, integrity and confidentiality of government data, the contractor shall afford the Government access to the contractor's facilities, installation, technical capabilities, operations, documentation, records and databases.
- If new or unanticipated threats or hazards are discovered by either the Government or the contractor, or if existing protections have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
- The contractor shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the contractor's computer facility, and the contractor will retain no NRC data within 30 calendar days after contract is completion. Until all data is purged, the contractor shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

- When contractor employees no longer require access to an NRC system, the contractor shall notify the project officer within 24 hours.
- Upon contract completion, the contractor 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.
- Any information made available to the contractor, in any format, shall be used only for carrying out the provisions of this contract. Information contained in such material shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Disclosure to anyone other than an authorized officer or employee of the contractor shall require written approval of the NRC Contracting Officer.
- The contractor 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 contractor under this contract or otherwise provided by the NRC.
- Contractors 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.
- All media used by the contractor to storing or processing NRC information must include appropriate markings to indicate the sensitivity of the information contained on the media and the media shall be controlled in accordance to the sensitivity level.
- The contractor 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 within 15 calendar days after being requested.
- For any contractor system used to process NRC information, the contractor 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 least every 7 calendar days.
- The contractor 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 contractor shall provide the system requirements traceability matrix at the end of the 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 contractor 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 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.

- The contractor 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 contractor 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.
- The contractor must ensure that all system modifications must comply with NRC Configuration Management policies and procedures.
- The contractor 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 contractor must have a configuration management plan that includes all hardware and software that is part of the system.
- 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 contractor shall not have the ability to make changes to the system's security posture without the appropriate involvement and approval of the ISSO.
- The contractor 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 contractor must maintain all system documentation that is current to within 30 calendar days.
- 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 contractor shall maintain a list of hardware, firmware and software changes that is current to within 30 calendar days.

- The contractor shall ensure that the development environment is separated from the operational environment using NRC CSO approved controls.
- The contractor shall only use licensed software and in-house developed authorized software (including NRC and contractor 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.
- The contractor shall provide proof of valid software licensing upon request of the Contracting Officer, the NRC Project Officer, a Senior Information Technology Security Officer, or the Designated Approving Authorities.
- 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.