AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO. | 1. CONTRACT ID CODE | PAGE 1 | OF PAGES 4

2. AMENDMENT/MODIFICATION NO. M015

3. EFFECTIVE DATE See Block 15C

4. REQUISITION/PURCHASE REQ. NO. DR-02-05-006

5. PROJECT NO.(If applicable)

6. ISSUED BY CODE 3100

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

7. ADMINISTERED BY (If other than Item 6) CODE 3100

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

Washington, DC 20555

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

OAO CORPORATION

7375 EXECUTIVE PLACE

SEABROOK MD 207062278

CODE DUNS: 074830209 FACILITY CODE

(X) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO. GS35F4524G DR-02-06-005

X 10B. DATED (SEE ITEM 13) 12-22-2005

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(X) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 3 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

See the attached continuation pages. DUNS: 074830209

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) Joyce L. Lambert Contract Management

16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Valerie M. Whipple Contracting Officer

15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)

15C. DATE SIGNED 8/21/2008

16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)

16C. DATE SIGNED 8/19/08

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

SEP 11 2008

ADM002

Contract No. DR-02-06-005 is hereby modified as follows:

- To revise the amount of Task 5 for the base period and each option period for an overall decrease in Task 5 of $1,315,207 should all Task 5 optional tasks be exercised;
- To decrease the delivery order amount by $1,039,171.84;
- To revise the Statement of Work to reflect changes made to the Task 5; and
- To replace the Alternate Project Officer with Melissa Ash.

Accordingly, the following changes are hereby made:

1. Attachment 1 of the delivery order, Schedule of Prices, is revised to delete the Task 5.1 table, and to replace Optional Task 5.2, Optional Task 5.3 and Optional Task 5.4 tables with the following tables:

Optional Task 5.2 - NSTS User Support
Period of Performance: 05/01/2008 - 12/31/2008

Category	Hours	Rate	Total
Project Manager	[redacted]	$	7,953
Principal Systems Architect	[redacted]	$	7,384
Principal Information Engineer	[redacted]	$	610
Senior Functional Analyst	[redacted]	$	27,562
Systems Analyst 5	[redacted]	$	32,444
Support Specialist 6	[redacted]	$	123,863
Support Specialist 5	[redacted]	$	3,947
Network Ops Specialist	[redacted]	$	6,282
TeleComm Eng - Inter	[redacted]	$	2,858
Total	[redacted]	$	212,903
Travel		$	2,094
H/W S/W ODC's		$	34,580
Total Price		$	249,577

Optional Task 5.3 - NSTS User Support
Period of Performance: 01/01/2009 - 12/31/2009

Category	Hours	Rate	Total
Project Manager	[redacted]	$	10,179
Senior Functional Analyst	[redacted]	$	14,934
Systems Analyst 5	[redacted]	$	10,034
Support Specialist 6	[redacted]	$	546,987
Network Ops Specialist	[redacted]	$	12,954
Total	[redacted]	$	595,088
Travel		$	2,166

H/W S/W ODC's	$	4,983
Total Price	$	602,236

Optional Task 5.4 - NSTS User Support
Period of Performance: 01/01/2010 - 12/31/2010

Category	Hours	Rate		Total
Project Manager	[redacted]		$	10,495
Senior Functional Analyst			$	15,396
Systems Analyst 5			$	10,345
Support Specialist 6			$	533,030
Network Ops Specialist			$	13,356
Total	[redacted]		$	582,623
Travel			$	-
H/W S/W ODC's			$	7,342
Total Price			$	589,965

2. Section B, CONSIDERATION AND OBLIGATION, Paragraphs (1) and (2) are hereby deleted in their entirety and replaced with the following [specific changes are identified in italics/bold]:

   (1) The total estimated amount of this order (ceiling) is ***$9,750,711.16*** which is comprised of Tasks 1, 3.1, 3.2, 4.1.1, 4.1.2, 5.1 and 5.2, as follows:

Base Period

Task 1	$5,905,507.00
Task 3.1	$2,029,424.00
Task 4.1.1	$ 308,673.92
Task 5.1	***$-0-***
	$ 8,243,604.92

Optional Period

Task 3.2	$ 800,000.00
Task 4.1.2	$ 457,529.24
Task 5.2	***$ 249,577.00***
	$1,507,106.24

Total Estimated Amount	***$9,750,711.16***

   (2) In the event that the Government exercises optional work pursuant to FAR Clause 52.217-8 and FAR Clause 52.217-9 incorporated in this delivery order, the total estimated amount of this order will increase as follows:

Optional Work under the Base Period

Optional Task 2	$1,697,201.14
Optional Task 4.2.1	$ 295,107.64

Optional Work under Option Period 1

Optional Task 4.2.2	$ 252,623.84

Optional Work under Option Period 2

Optional Task 3.3	$1,165,000.00
Optional Task 4.1.3	$ 478,590.40
Optional Task 4.2.3	$ 259,624.24
Optional Task 5.3	***$ 602,236.00***

Optional Work under Option Period 3

Optional Task 3.4	$1,182,828.00
Optional Task 4.1.4	$ 493,430.40
Optional Task 4.2.4	$ 266,488.08
Optional Task 5.4	***$ 589,965.00***

3. The attached Schedule II-A Equipment under Task 5, is hereby added to the contract as Attachment 8.

4. To revise Section H. Project Officer to replace Paul Goldberg with Melissa Ash as the Alternate Project Officer. Ms. Ash' contact information is as follows:

Alternate Project Officer: Melissa Ash
FSME/PBPA/IT
O-8A23
301-415-7851
Melissa.Ash@NRC.GOV

This modification does **not** obligate FY'08 funds.

Except as provided herein, all other terms and conditions remain unchanged and in full force and effect.

ATTACHMENT 5
DR-02-06-005

SafeSource Phase II
Performance Based Statement of Work (PBSOW)

Revised August, 2008

Deleted: April

Table of Contents

1. INTRODUCTION 1

1.1 Overview 1

1.2 Background 1

1.3 Objectives 3

2. SCOPE 4

2.1 Scope Included 4

2.2 Scope Exclusions 6

2.3 Scope of Interaction with Concurrent Projects 6

3. NSTS SYSTEM REQUIREMENTS 6

3.1 Overview 6
System Concept 6
Operational Architecture 8
System Interfaces 11

3.2 Functional Requirements 11
3.2.1 Licensee Requirements 11
3.2.2 Licensing Agency Requirements 15
3.2.3 System Administration Requirements 18
3.2.4 System Timer Requirements 20

3.3 Performance Requirements 21
3.3.1 External Workloads 21
3.3.2 Throughput, Response Times, and Internal Function Workload 21
3.3.3 Data Quality, Integrity, and Accuracy 22
3.3.4 Data Retention, System Capacity, and Communications Capacity 22
3.3.5 Reliability, Maintainability, and Availability 22
3.3.6 Growth, Flexibility, and Expandability 22
3.3.7 Backup and Recovery 23

3.4 Operational Requirements 23
3.4.1 Human Factors 23
3.4.2 Facilities, Environment, Safety, System Monitoring, and Support Capabilities 24
3.4.3 Configuration Control 24
3.4.4 Security 24
3.4.5 Documentation 25

3.5 Programmatic Requirements 26
3.5.1 Development Facilities and Support Requirements or Constraints 26

3.6 Data Requirements 26

4. WBL SYSTEM REQUIREMENTS – OPERATIONAL SUPPORT AND MAINTENANCE 28

4.1 Overview 28
System Concept 28
Operational Architecture 29
System Interfaces 31

4.2 Functional Requirements 32

4.3 Performance Requirements 32
4.4 Operational Requirements 32
4.5 Programmatic Requirements 32
4.6 Data Requirements 32
5. CONTRACTOR PERFORMANCE REQUIREMENTS 34
5.1 Overview 34
5.2 Methodology Compliance 38
5.3 Task 1: Establish Initial NSTS 38
Scope of Work 38
Schedule and Detailed Task Descriptions 38
Deliverables 48
5.4 Optional Task 2: Develop Enhanced NSTS 51
Scope of Work 51
Schedule and Detailed Task Descriptions 51
Deliverables 56
5.5 Task 3: Operational Support 57
5.5.1 Task 3.1 Operational Support for the NSTS and WBL – Base Period 57
5.5.3 Optional task 3.2 Operational Support for the NSTS and WBL – Option Period 1 60
5.5.4 Optional task 3.3 Operational Support for the NSTS and WBL – Option Period 2 60
5.5.5 Optional task 3.4 Operational Support for the NSTS and WBL – Option Period 3 61
5.6 Task 4: Maintenance 61
5.6.1 Task 4.1 NSTS Maintenance 61
Task 4.1.1 NSTS Maintenance – Base Period 61
Optional task 4.1.2 NSTS Maintenance – Option Period 1 61
Optional task 4.1.3 NSTS Maintenance – Option Period 2 61
Optional task 4.1.4 NSTS Maintenance – Option Period 3 62
5.6.2 Task 4.2 WBL Maintenance 62
Optional task 4.2.1 WBL Maintenance – Base Period 62
Optional task 4.2.2 WBL Maintenance – Option Period 1 63
Optional task 4.2.3 WBL Maintenance – Option Period 2 63
Optional task 4.2.4 WBL Maintenance – Option Period 3 63
5.7 Task 5: NSTS User Support 63
Task 5.1 NSTS User Support – Base Period 63
Optional task 5.2 NSTS User Support – Option Period 1 ....65 Deleted: 64
Optional task 5.3 NSTS User Support – Option Period 2 ....65 Deleted: 64
Optional task 5.4 NSTS User Support – Option Period 3 65
6. TECHNICAL ENVIRONMENT 65
6.1 SafeSource Phase I Technical Architecture 65
6.1.1 LicenseEase Architecture 65
6.1.2 eGateway Architecture ....66 Deleted: 65
6.2 SafeSource Phase II Technical Architecture 66
6.3 SafeSource Infrastructure and Operational Requirements ....68 Deleted: 67
6.3.1 Multi-Tiered Infrastructure ....68 Deleted: 67
6.3.2 Application Service Provider 68
6.3.3 Telecommunications ....69 Deleted: 68
6.3.4 Security ....70 Deleted: 69

6.3.5 Development Environment ..... 70 Deleted: 69
6.3.6 Testing and Production Environments ..... 70 Deleted: 69
6.4 Existing NRC Infrastructure and Operations ..... 70 Deleted: 69
6.4.1 Compatibility During Development 70
6.4.2 Compatibility In Production Deployment 71
6.5 Government Furnished Equipment ..... 72 Deleted: 71
6.6 Compliance with the NRC System Development Methodology ..... 73 Deleted: 72
7. DESIGN AND IMPLEMENTATION CONTROLS ..... 73 Deleted: 72
7.1 General Design and Implementation Controls ..... 73 Deleted: 72
7.2 Detailed Design and Implementation Controls for Security 73
7.3 Detailed Controls for Engineering, Development, and Testing ..... 77 Deleted: 76
7.4 Engineering the Solution ..... 78 Deleted: 77
7.5 Detailed Controls for Training ..... 81 Deleted: 80
7.6 Detailed Controls for Ongoing Support ..... 82 Deleted: 81
8. ORDER TERMS, CONDITIONS, AND REQUIREMENTS ..... 82 Deleted: 81
8.1 Performance Requirements ..... 82 Deleted: 81
8.2 Place of Performance 82
8.3 Travel 82
8.4 Reporting Requirements ..... 83 Deleted: 82
8.5.1 Weekly Reports and Meetings ..... 83 Deleted: 82
8.5.2 Project Management Plan ..... 83 Deleted: 82
8.5.3 Monthly Reports and Meetings 83
8.5.4 Provide Data for Earned Value Reporting ..... 84 Deleted: 83

Appendices

A. Performance Requirement Summary
B. Requirements Analysis for SafeSource Phase II: National Source Tracking System
C. Management Directive 3.14
D. PMM Schedule Template for Task 1
E. PMM Software Development Plan Template
F. PMM Quality Assurance Plan Template
G. PMM Deployment Plan Template
H. PMM System Architecture Document Version 1
I. Detailed Design Standards
J. NMSS COTS Policy
K. NRC Risk Assessment Report Template
L. NRC Security Plan Template
M. NRC Contingency Plan Template
N. PMM Test Plan Template
O. PMM Test Evaluation Summary Template
P. PMM Schedule Template for Task 2
Q. OCIO Application Change Request System Guide
R. Functional Testing Standards
S. Earned Value Reporting Technical Guide
T. RSRT Evaluation Summary

1. INTRODUCTION

1.1 Overview

SafeSource is the overall name for a project that provides Information Technology (IT) support for the Nuclear Regulatory Commission's initiative to improve licensing and security of nuclear materials. A major impetus for SafeSource is the need to control nuclear materials that could be used in a radiological dispersal device (RDD) or "dirty bomb" – a conventional explosive that carries nuclear materials and releases them on detonation.

The NRC has established a two-phase strategy for implementing SafeSource:

- SafeSource Phase I is establishing NRC experience with the technology platform selected for the entire SafeSource initiative. This project is utilizing this back-end infrastructure and a commercial off-the-shelf (COTS) front end to provide a new licensing and inspection system that will replace three legacy systems while providing improved integration and functionality.

- SafeSource Phase II will implement national, centralized, nuclear source tracking—a requirement now being written into NRC regulation. This requirement will be for all U.S. nuclear materials licensees to report and track individual nuclear sealed sources that contain "materials of greatest concern". Tracking will span the entire life-cycle of each source – manufacture or import, receipt, transfer, and an end point, such as export or burial.

This Performance Based Statement of Work (PBSOW) for SafeSource Phase II includes development of the National Source Tracking System (NSTS). It also includes operational support for the entire SafeSource infrastructure, maintenance and user support for the NSTS, and optional maintenance for the Web-based Licensing System (WBL). The WBL is being developed under a separate contract.

The sponsoring office for this project, the Office of Nuclear Material Safety and Safeguards (NMSS), conducted a comprehensive analysis to examine alternative solutions and has chosen an approach to develop the NSTS, as a custom system which operates in a technical infrastructure similar to that of the WBL and which uses a commercial Application Service Provider (ASP) whose core competency is Web-based secure systems. As an extension to the NSTS alternatives analysis, NMSS performed a detailed evaluation of the DOE Radiological Source Registry Tracking (RSRT) system. A summary of the findings of this evaluation is included in Appendix T.

1.2 Background

The events of September 11, 2001 heightened the nation's concern regarding the use of radioactive materials for a malevolent act. The potential for such an attack has been of particular concern because of the widespread use of radioactive materials (often contained in sealed sources) in the United States and abroad by industry, hospitals, and academic institutions.

In July 2002, the Nuclear Regulatory Commission (NRC) and the Department of Energy (DOE) established an RDD Working Group to investigate how to improve the control of nuclear

material or radioactive sources. One recommendation of the RDD Working Group, as documented in its May 2003 report, was to develop a national source tracking system to better understand and monitor the location and movement of sources of interest[1]. In order to track source transfers in a timely manner, the RDD Working Group recommended that the system be Web-based, allowing most source transactions to be recorded directly by licensees using the Internet. During the summer of 2003, the NRC adopted this recommendation and directed its staff to begin regulatory and development activities on a national source tracking system.

The NRC has also supported the latest revision to the International Atomic Energy Agency (IAEA) "Code of Conduct on the Safety and Security of Radioactive Sources" (Code of Conduct), approved in September 2003. The Code of Conduct calls for the establishment, by 2007, of national registers of radioactive sources that pose the most significant risks. Although the Code of Conduct is not an international treaty, and its provisions are non-binding, the NRC nevertheless believes it is essential to enact its recommendations. In early 2004, the NRC made a commitment to Congress to develop source tracking regulations as envisioned in the IAEA Code of Conduct[2].

The NRC began activities needed to develop the NSTS in late 2003. Recognizing that the NSTS would be a collaborative effort involving multiple federal and state agencies, NRC established a governance and project structure with representation from significant government stakeholders:

- **The SafeSource Steering Committee** has NRC, DOE and Agreement State representation. It is tasked with policy direction and oversight of the SafeSource Phase II--NSTS Working Group, and the SafeSource Phase I--Web-based Licensing Working Group.

- **The SafeSource Phase I--The Web-based Licensing Group** has representation from NRC Headquarters and Regions, as well as the Agreement States. It prepared the WBL requirements and is contributing to the implementation of the ongoing SafeSource Phase I system development effort.

- **The SafeSource Phase II--NSTS Working Group** has NRC, DOE and Agreement State representation and is tasked with preparing NSTS system requirements, recommending the necessary regulatory changes, providing input to the business case, and contributing to the development and implementation efforts.

[1] NRC and its 33 Agreement States issue licenses for the medical, industrial, and academic uses of nuclear materials within their separate jurisdictions. Current federal and state regulations do not require centralized registering or tracking of nuclear sources. No central database currently exists for high-risk sources in the United States.

[2] Congress and the Government Accountability Office (GAO) have expressed interest in a National Source Tracking System. The Energy Policy Act of 2005 requires NRC to issue regulations establishing a radiation source tracking system. Several GAO reports have recommended tighter federal control of the security of radioactive sources.

- **The NSTS Interagency Coordinating Committee** has NRC, DOE, and Agreement State representation, as well as representation from the following federal agencies:
  - Department of State (DOS)
  - Department of Transportation (DOT)
  - Department of Commerce (DOC)
  - Department of Defense (DoD)
  - Department of Justice, Federal Bureau of Investigation (FBI)
  - Department of Homeland Security, Infrastructure Protection (DHS/IP)
  - Department of Homeland Security, Customs and Border Patrol (DHS/CBP)
  - Department of Homeland Security, Transportation Security Administration (DHS/TSA)
  - Environmental Protection Agency (EPA)

  This committee provides guidance regarding interagency issues associated with the development of the NSTS.

1.3 Objectives

Once operational, the NSTS must provide a full life cycle account of the origins of each source of concern (manufacture, recycling, or import) and record by whom, when, and where it has been transported, possessed, and eventually disposed of or exported.

The NSTS will satisfy the IAEA Code of Conduct's call for a national, central database of high-risk sources, and will help the NRC and other agencies:

- monitor the location, possession and disposal of radioactive sources of concern throughout the country;
- improve accountability and give better information to decision makers;
- detect and act on tracking discrepancies;
- conduct inspections and investigations;
- communicate radioactive source information among government agencies;
- respond in the event of an emergency;
- verify legitimate import, export, ownership, and use of radioactive sources; and
- further analyze hazards attributable to the possession and use of radioactive materials.

The NSTS will be designed to:

- be primarily Web-based;
- include nuclear sources of highest concern from NRC and Agreement States licensees and DOE facilities;
- require licensees and facilities to report the manufacture, transfer, receipt, and disposition of sources; and
- minimize impact on licensees to the extent practical.

2. SCOPE

2.1 Scope Included

This PBSOW includes phased development, training, and deployment of the NSTS, and operational support, maintenance, and user support at appropriate points in the project. The operational support, maintenance, and user support tasks cover a broad range of activities including:

- database and application hosting for the NSTS;
- database and application hosting for the WBL;
- maintenance of all NSTS infrastructure that is external to the NRC headquarters campus, excluding software and hardware required for users to establish internet connections, set-up and recurring costs of telecommunication lines, services, and infrastructure;
- maintenance of all WBL infrastructure that is external to the NRC headquarters campus, excluding software and hardware required for users to establish internet connections, set-up and recurring costs of telecommunication lines, services, and infrastructure;
- database and application software maintenance for the NSTS and WBL.; and
- comprehensive user support.

The SafeSource Phase II PBSOW is divided into the following five tasks:

- **Task 1: Establish Initial NSTS. (Base Period)** NSTS Release 1 (V1) will provide the basic Web-based functionality needed to meet the new NRC source tracking regulations and the IAEA Code of Conduct requirements for source registry.

  NSTS V1 will be accessible to limited NRC, DOE, and Agreement State (A/S) personnel and will be deployed to affected nuclear materials licensees in two phases. Each deployment group will comprise a "supply chain" of manufacturer/distributors, source users, and disposers, so that sources can be tracked through their life-cycles within that group.

Task 1 includes support for public workshops to familiarize affected licensees with use of the NSTS.

- **Optional Task 2: Enhanced NSTS. (Base Period)** Should the NRC exercise this option, the enhanced system will implement the following functionality:
    - the ability for NRC to record and track import consents and import/export notifications made by NRC import/export licensees;
    - the ability to link notifications to import and export transfer and receipt transactions, and report import and export related information;
    - provide notifications required by DHS/Customs and Border Protection (CBP); and
    - automated system interfaces, full reporting and alert capabilities, and reporting to additional federal agencies.

  Functionality implemented in Task 2 will be deployed to all affected licensees simultaneously.

- **Task 3: Operational Support.**
    - **Task 3.1 Operational Support for the NSTS and WBL – Base Period**
    - **Optional task 3.2 Operational Support for the NSTS and WBL – Option Period 1**
    - **Optional task 3.3 Operational Support for the NSTS and WBL – Option Period 2**
    - **Optional task 3.4 Operational Support for the NSTS and WBL – Option Period 3**
- **Task 4: Maintenance.**
    - **Task 4.1 NSTS Maintenance**
        - **Task 4.1.1 NSTS Maintenance – Base Period**
        - **Optional task 4.1.2 NSTS Maintenance – Option Period 1**
        - **Optional task 4.1.3 NSTS Maintenance – Option Period 2**
        - **Optional task 4.1.4 NSTS Maintenance – Option Period 3**
    - **Task 4.2 WBL Maintenance**
        - **Optional task 4.2.1 WBL Maintenance – Base Period**
        - **Optional task 4.2.2 WBL Maintenance – Option Period 1**
        - **Optional task 4.2.3 WBL Maintenance – Option Period 2**
        - **Optional task 4.2.4 WBL Maintenance – Option Period 3**

- **Task 5: NSTS User Support.**

- **Task 5.1 NSTS User Support – Base Period**
- **Optional task 5.2 NSTS User Support – Option Period 1**
- **Optional task 5.3 NSTS User Support – Option Period 2**
- **Optional task 5.4 NSTS User Support – Option Period 3**

All five tasks will have performance requirements, incentives, and disincentives as described in the Performance Requirement Summary (PRS) attached in Appendix A. The schedule, activities, and deliverables for these tasks are covered in more depth in Section 4 of this PBSOW.

2.2 Scope Exclusions

This PBSOW does not cover:

- WBL activities or costs incurred during WBL development and implementation phases (SafeSource Phase I);
- maintenance of any Versa-proprietary aspects of the base WBL COTS products, LicenseEase and eLicense Gateway (Note: support for configuration, extension, management, and administration (e.g., access rights) related to the COTS products **are within scope**);
- NRC staff and NRC IV&V Contractor costs for NSTS; or
- support of DOE efforts to upgrade their existing source inventory system so that it captures the tracking information needed for entry into NSTS.

2.3 Scope of Interaction with Concurrent Projects

WBL will become operational in late 2005 under the SafeSource Phase I contract. The NRC plans to transfer WBL operations to the SafeSource Phase II ASP sometime between the SafeSource Phase II contract award and the summer of 2006. Transition activities are included in Task 3.1 Operational Support for NSTS and WBL System – year 1.

3. NSTS SYSTEM REQUIREMENTS

The requirements presented in this section are a summary of the detailed requirements found in the Appendix B: SafeSource Phase II Requirements Analysis.

3.1 Overview

This section provides a high-level description of the NSTS in terms of its overall system concept, its operational architecture, and its interfaces with external systems.

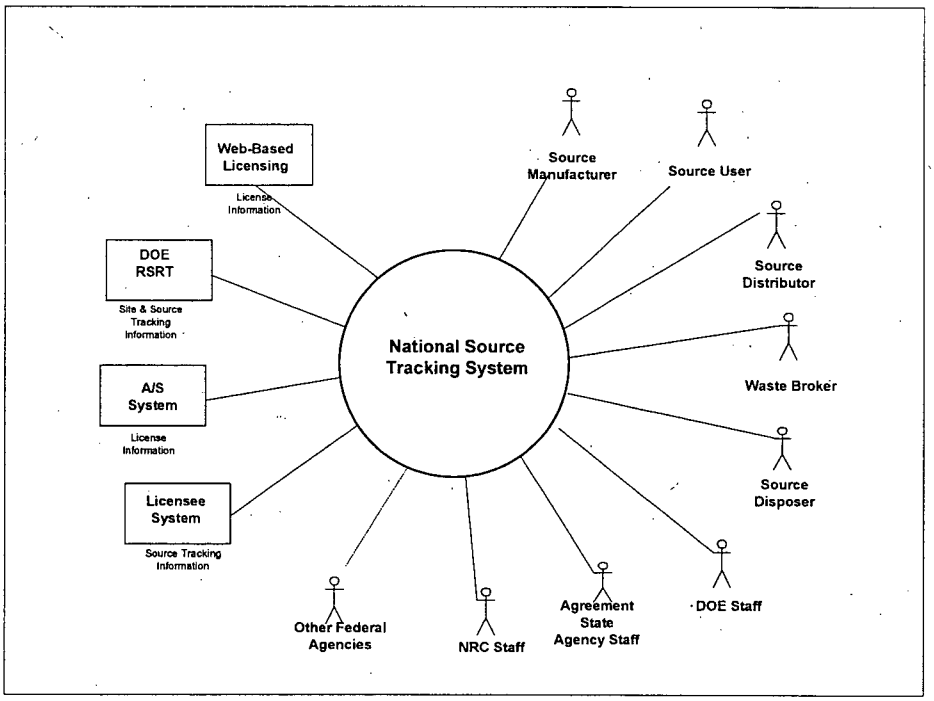
System Concept

The NSTS will track the manufacture, possession and transfer of individual nuclear sealed sources by U.S. nuclear materials and import/export licensees throughout their entire life-cycle. The major functions of the system include the following:

- the ability to record information about individual sealed sources including important source characteristics such as: make, model, serial #, isotopes, activity, activity date, and status;
- the ability to record the list of individual sources that are currently associated with each license (an inventory);
- the ability to track the transfer of possession of an individual source from one licensee to another and from one status to another (e.g., 'active' to 'lost');
- the ability to see a full history of transfers and status changes for an individual source;
- the ability for NRC licensees, Agreement State licensees, and DOE sites to record in a timely manner, source characteristics, source transfers, and source status changes;
- the ability for the licensing agencies (NRC, Agreement State agencies, and DOE) to establish and maintain the license information of their respective jurisdictions, including the ability to record source incidents such as: lost, stolen, destroyed, irretrievable, and found sources;
- the ability to import data files submitted by licensees and other stakeholders;
- the ability to schedule and generate both pre-programmed and ad-hoc reports, to upload electronic files of source and license information from external systems, and to extract source information for use by other federal agencies; and
- the ability to provide event monitoring and alert notifications to enhance the timely reporting and monitoring of NSTS data integrity.

Exhibit 3-1 shows the major classes of users and the system interfaces that form the context for the NSTS.

Exhibit 3-1: NSTS System Context



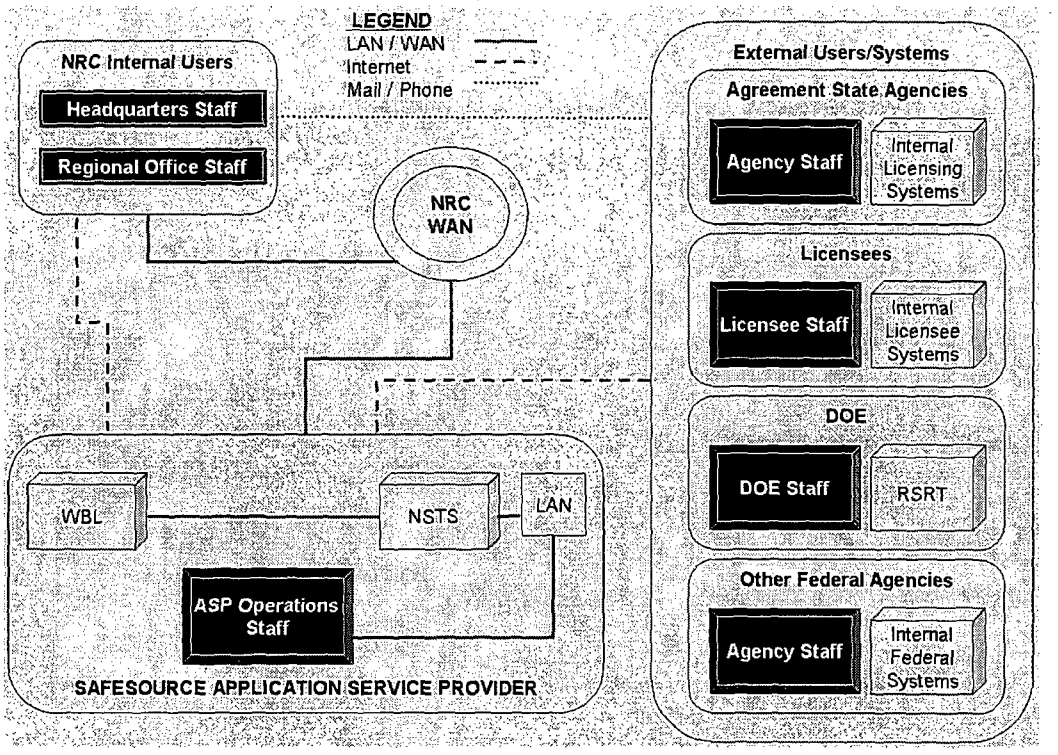
The Context Diagram above shows direct users of the NSTS (shown as stick figures) and automated systems (shown as rectangles) that will interface with NSTS. The system will provide a central, Web-based platform that can be accessed by affected nuclear materials licensees nationwide. These include nuclear source manufacturers, source distributors, source users, waste brokers and source disposers. The NSTS will also be accessible via the Web to appropriate staff members of the NRC, NRC Agreement State agencies, and the DOE. Additional indirect users will include appropriate staff from other federal agencies such as: the Department of Homeland Security (DHS), U.S. Customs and Border Protection bureau (DHS/CBP), Department of Transportation, Department of Defense, Environmental Protection Agency, Department of State, and Department of Commerce.

The NSTS must interface with numerous existing systems. It will receive updates from the NRC WBL as well as the DOE Radiological Source Registry Tracking (RSRT) system, Agreement State agency licensing systems, and licensee inventory systems. The NSTS will also provide data to external entities such as the Department of Homeland Security and other federal agencies.

Operational Architecture

The NSTS will use some components of and build upon the architecture already specified for the SafeSource Phase I project. These architectural constraints include use of a commercial ASP, the Oracle application server / database technology, and Virtual Private Network (VPN) technologies. Exhibit 3-2 presents a conceptual top-level system view for the NSTS.

Exhibit 3-2: NSTS Conceptual Top-Level System View



An ASP will host both the NSTS and the WBL. The SafeSource operational environment provided by the ASP will include:

- Internet connectivity;
- secure Web-Based front-end with back-end data base and processing applications;
- separate development, test, and production environments;
- backup and recovery;
- intrusion detection;
- firewall capabilities;
- security-data and privilege restrictions; and
- interfaces with applications hosted on NRC and DOE platforms.

The NSTS will use the same Oracle application server and database platforms that have been established for the WBL. The NRC expects that this common platform will provide cost savings related to database licenses, database administration support, and system administration support. The NSTS database itself will be implemented as a separate instance from the WBL database instance. The database software licenses will be provided by the NRC.

NRC users will access the NSTS using a high speed connection compliant with specifications found in Section 6.3.3 and other requirements expressed in this document and Appendix B. After transition of the WBL to the NSTS ASP, the NRC will access both systems using the same high speed connection. External users, including Agreement State agencies, licensees, DOE, and other federal agencies will access the system using their local Internet connectivity. The SafeSource Phase II Contractor will provide ongoing support to any external users who choose to interact via telephone, by mailing paper-based transactions, or in using the NSTS.

Interfaces will be established to facilitate the batch loading of data into the NSTS. This will enable license data to be received from the NRC WBL and the Agreement State (A/S) agency licensing systems. It will also enable source transaction data to be received from licensees and the DOE. An interface will also be established to provide data extracts of some or all of the NSTS information for use by other federal agencies to perform additional analysis based on their specialized needs.

The NSTS user community will consist of NRC, A/S agencies, DOE, other federal agencies, contract personnel, and licensees with varying, role-based capabilities within the system. The hardware/software configuration and cost estimates for the SafeSource Phase II alternatives are based on the following numbers of users:

Organization(s)	Entry Users	Read-Only	Total Users
NRC/Headquarters	12	28	40
NRC/Regions--Entry	4	0	4
NRC/Regions--Inspectors	0	41	41
NRC/Regions--Management	0	18	18
A/S Agencies	40	40	80
NRC and A/S Licensees	20,000	0	20,000
DOE Headquarters	5	10	15
Additional Federal Users	0	50	50
Contractor Analysts	6	0	6
Contractor IT Support	15	0	15
Contractor IV&V	4	0	4
TOTAL	20,086	187	20,273

The NRC users will receive specific training in the use of the NSTS. DOE and Agreement State users may request to participate in the training session conducted in the NRC facilities. Additionally, at least one training session will be presented at the Organization of Agreement States meeting. Non-NRC users will have the opportunity to attend workshops and receive computer-based-training (CBT). The CBT portfolio will include role-based modules addressing all functions of the Licensee and Licensing Agency user communities. The NSTS web interface

will include user-friendly navigation tools, online help, and other aids to facilitate access by all users.

System Interfaces

Batch upload interfaces will be established for loading data from various internal and external systems, which include:

- the Web-based Licensing System (WBL) – provides NRC license data;
- Agreement State licensing systems – provides Agreement State license data;
- the Radiological Source Registry Tracking System (RSRT) of DOE – provides DOE Site information and source data; and
- licensee systems – provides individual licensee's source tracking data.

The NSTS will also provide batch extract data to external entities such as the Department of Homeland Security and other federal agencies.

3.2 Functional Requirements

The Functional Requirements define the intended behavior of the system from the NRC business point of view. They describe what actions and processes will exist in the system and how they will behave.

The functional requirements have been documented using industry standard, object-oriented analysis and design techniques. In particular, the Unified Modeling Language (UML) 'use-case' technique has been used to elicit and document the functional requirements of the system. The use-case technique is a way of describing the behavior of a system from the viewpoint of the users that interact with the system.

The use-case specification is a textual description of each use case (functional process) in the diagram. The requirements listed in this section are a summary of the detailed use case diagrams and specifications that are listed in Appendix B, SafeSource Phase II Requirements Analysis[3]. Requirements have been grouped into four major functional areas: Licensee functions, Licensing Agency functions, System Administration, and System Timer.

3.2.1 Licensee Requirements

The Licensee functional area contains requirements that primarily support the Licensee's source tracking activities. A Licensing Agency can also access these functions on behalf of its licensees.

Manufacture New Sources (UC1)

This use case enables a Source Manufacturer to record the manufacturing or re-manufacturing of new sources. This is a starting point ("birth") of a trackable source's life-cycle. The

[3] A use case identifier appears in parenthesis at the end of each requirement name, as an easy reference to the full use case specification details located in the appendix.

mandatory information recorded about each source includes: make/model, serial number, isotope, activity, activity unit, activity date, manufacture date, and primary location. The source identification number and the manufacturer's license information will be automatically associated with each source entered. Other optional information about a source may also be recorded.

Regenerate Sources (UC2)
This use case enables a Source Manufacturer to record when a source's activity amount has been increased through a 'regeneration' process. The user will be able to search for a specific source and for each of the source's isotopes and will be able to enter new values such as: activity, activity unit, activity date, regeneration date, and comment.

View Transfer Progress (UC3)
This use case enables an authorized user to view information about a chosen shipment and its associated source transfers. Licensees will only be able to view transfers to which they are a party—either as the sending or receiving licensee. In general, Licensing Agencies will only be able to view transfers to which at least one of their licensees is a party.

Transfer Sources (UC4)
This use case enables a Licensee to record the transfer of one or more of its sources to another U.S. nuclear materials licensee (and appropriate DOE facilities). The Licensee will be presented with a list of the sources in its inventory and prompted to select which sources to include in the transfer. If the sources are to be sent to a disposer, the user can enter the Container IDs and the Manifest Number. A transfer identification number and the license information of both sending and receiving licensees will be automatically associated with the transfer.

Export Sources (UC5)
This use case enables a Licensee to record the export of one or more of its sources to a foreign recipient. The Licensee will be presented with a list of the sources in its inventory and prompted to select which sources to include in the export. The user will also be able to search for and associate this export with a previously entered Export Notification.

Update/Cancel Source Transfers (UC6)
This use case enables a Licensee to update or cancel a chosen transfer for which it is the 'Sending Licensee'. For example, a Source Manufacturer may need to correct the recipient of a transfer because it was previously entered incorrectly or may need to cancel a transfer because the source was mistakenly included in a shipment.

Verify Pending Transfers (UC7)
This use case enables a Licensee to confirm or reject a pending shipment/transfer for which it is the 'Sending Licensee'. The need for this function arises when a Receiving Licensee receives a source whose transfer was not in the system. The Receiving Licensee must therefore enter the source transfer into the system on behalf of the 'Sending Licensee' in order to receive it. The entered transfer is automatically marked by the system as a 'pending' transfer. The Sending Licensee must then confirm or reject 'pending' transfer.

Review Transfer History (UC8)
This use case enables an authorized user to view and print a history of a chosen licensee's transfers, receipts, imports, and exports. Transfer information will include detailed information about each source included in each transfer, transfer and receipt dates, sending and receiving

licensee name and address, and transfer status (e.g., pending, received, received—incomplete, and overdue.) Associated import and export notifications will also be indicated.

Receive Sources (UC9)

This use case enables a Licensee to record the receipt of a shipment of sources from another U.S. nuclear materials licensee. The user will be presented with a list of pending domestic shipments for which the licensee is the intended recipient and prompted to select which transfer is being received. The user will then be presented with a list of the sources in the shipment, and prompted to verify the receipt of each source. The user will also be able to indicate receipt of an incomplete shipment, or enter a pending transfer if no matching transfer is found in the system. The user will select or enter the primary location where each source will be stored.

Receive Imports (UC10)

This use case enables a Licensee to record the receipt of an imported shipment of sources from a foreign entity. The user will be presented with a list of any pending import consent/notifications for which the licensee is the intended recipient and prompted to select which import is being received. If the import notification lists individual sources, the user will be presented with a list of these sources and prompted to verify the receipt of each. If the import shipment does not list sources, the user will be able to enter records for the sources in the shipment.

Record Source Location (UC11)

This use case enables a Licensee to record a new primary location of a chosen source. The term 'primary location' (a.k.a. 'home base') refers to the address where the source is typically kept.

View Own Inventory (UC12)

This use case enables a Licensee to sort and display a list of sources that are considered by NSTS to be in its possession. The system will display information such as: make/model, serial number, source id, isotope, activity, activity unit, activity date, acquisition date, location address, device make, device model, device serial number, comment, etc.

Verify Annual Source Inventory (UC13)

A periodic verification and reconciliation of NSTS inventory against physical inventory will be required. This use case enables a Licensee to enter inventory verification information. The Licensee will be presented with a list of the sources in its NSTS inventory grouped by location address. Licensees will be required to make any corrections to the inventory through other use cases, such as "Enter Unrecorded Sources". When satisfied with the verification, the user will be able to submit it electronically to the system.

Specify Long-Term Storage Sources (UC14)

This use case enables a Licensee to record when a source in the licensee's inventory is no longer in use. This would include sources that cannot be disposed of (e.g., Greater Than Class C.) Such sources are said to be in long-term storage.

Update Source Information (UC15)

This use case enables a Licensee to update and correct information about a source in the licensee's inventory. This information may include: make/ model, serial number, isotope,

activity, activity unit, activity date, device make/model, device serial number, primary location address.

Enter Unrecorded Sources (UC16)

Licensees and Licensing Agencies need to proceed with source reporting/recording activities, such as transfer and receipt, even if a source has not been previously recorded in NSTS (i.e., an "unrecorded source"). This use case enables an authorized user to enter an unrecorded source during appropriate NSTS transactions. Recording an unrecorded source generates an alert which is delivered to the designated Agency Staff. (See use case "Generate Alerts").

Enter Unrecorded Transfers (UC17)

Licensees and Licensing Agencies need a way to enter receipt of a source transfer even if its originating transfer has not been previously recorded in NSTS (i.e., an "unrecorded transfer"). This use case enables a Receiving Licensee to enter an unrecorded transfer when that transfer is not found in NSTS. Once the unrecorded transfers are entered, the Receiving Licensee can proceed to complete the receipt of sources through the use case "Receive Sources".

Enter Unrecorded Locations (UC18)

Licensees and Licensing Agencies need a way to enter a location that has not previously been recorded in NSTS (i.e., an 'unrecorded location'). This use case enables an authorized user to enter an unrecorded location when that location is not found in NSTS. Recording an unrecorded location generates an alert which is delivered to the designated Agency Staff for follow-up (see use case "Generate Alerts").

Enter Unrecorded Make/Model (UC19)

Licensees and Licensing Agencies need a way to enter a source make/model or a device make/model that is not already recorded in the NSTS (i.e., an 'unrecorded make/model'). This use case enables an authorized user to enter an unrecorded make/model when that make/model is not found in NSTS. Recording an unrecorded make/model generates an alert which is delivered to the designated Agency Staff for follow-up (see use case "Generate Alerts").

Enter Unrecorded Licensees (UC20)

Licensees and Licensing Agencies need a way to enter information about a licensee that was not previously recorded in NSTS (i.e., an 'unrecorded licensee'). This use case enables an authorized user to enter an unrecorded licensee when that licensee is not found in NSTS. Recording an unrecorded licensee generates an alert which is delivered to the designated Agency Staff or Contractor for follow-up (see use case "Generate Alerts").

Dispose of Sources (UC21)

This use case enables a Source Disposer to record the disposal (e.g., burial) of sources that it has received. The Source Disposer will be able to search for and select one or more source containers in its inventory to dispose of and will be able to record a disposal date and optional disposal comment with each source Container.

Obtain Supporting Information (UC22)

This use case enables an authorized user to access a list of reference documents (including other websites) that are related to NSTS. Examples include: NSTS Frequently Asked Questions; the regulations governing source tracking requirements; guidance on the use of

NSTS; the IAEA (International Atomic Energy Association), DOE, and NRC home pages.

Send a Message to NSTS Mailbox (UC23)

This use case enables an authorized user to send a message to the NSTS Mailbox from various places in the system. The Mailbox will be managed by one or more designated NRC staff members or contract personnel

3.2.2 Licensing Agency Requirements

The Licensing Agency functional area contains requirements that primarily support the Licensing Agencies' activities.

Create Licenses (UC24)

This use case enables an authorized user to enter a new license into the system. This includes licenses for possession, import, and export of nuclear material. The authorized users include NRC Staff, Agreement State Staff, and Master Materials Licensees (MML). An MML would use this function to add a new permittee as a 'pseudo-license' that would automatically be associated with the parent MML. Creating a new license generates a 'New User Account' alert which is delivered to the designated Agency Staff for follow-up (see use case "Generate Alerts").

Update/Delete License Information (UC25)

This use case enables an authorized user to update license Information in the system or delete a license from the system. The authorized users include NRC Staff, Agreement State Staff, and Master Materials Licensees (MML). The system will allow a license to be deleted only if there is no open transfer for the licensee (i.e., only 'Completed' or 'Cancelled' transfers) and the licensee does not possess any sources that have not reached an end-point.

Record Destroyed Sources (UC27)

Sources are disassembled and reassembled as part of the "re-manufacturing" process that some Manufacturers perform. This disassembly process effectively means that the original source is "destroyed". A source may also be destroyed as a result of an accident. The Licensee must report to its Licensing Agency when an NSTS trackable source is destroyed. This use case enables the Licensing Agency to record that a source has been 'destroyed' as a result of an accident or a re-manufacturing process.

Record Lost or Stolen Sources (UC28)

A Licensee must report to its respective agency (the NRC, Agreement States, or DOE) when sources are lost or stolen. This use case enables a Licensing Agency to record that a source has been reported as lost or stolen by a licensee. The Licensing Agency will be able to search and select the source in the reporting licensee's NSTS inventory, and record information such as: source status (lost or stolen), incident report number, the date the source was reported lost or stolen, and comments. Recording a lost or stolen source generates an alert which is delivered to the designated Agency Staff (see use case "Generate Alerts").

Record Found Sources (UC29)

A Licensee or a member of the public may report to the NRC, Agreement States, or DOE that a source is found. This is typically entered via the NRC operations call center or Agreement State/DOE equivalents. This use case enables a Licensing Agency to record that a source has

been reported found by a licensee or member of the public. The Licensing Agency will be able to search and select the source, including those previously reported lost or stolen, and record information such as: source status (found), the date and place the source was found (discovery date), its current location, and comments. Recording a found source generates an alert which is delivered to the designated Agency Staff (see use case "Generate Alerts").

Record Irretrievable Sources (UC30)

A Licensee must report to its respective agency (the NRC, Agreement States, or DOE) when a source is irretrievable. This is typically entered via the NRC Operations Center or the Agreement State / DOE equivalents. This use case enables a Licensing Agency to record that a source has been reported as irretrievable by a licensee. The Licensing Agency will be able to search and select the source in the licensee's NSTS inventory, and record information such as: source status (irretrievable--end point of source), the date the source became irretrievable, and the Location of Abandonment.

Review Inventory Verifications (UC31)

This use case enables a Licensing Agency to view and print a status report of licensees' inventory verifications within a specified timeframe. The user will be able to search for and display information for one or more licensees, the date of their last verifications, and the status of their current verification. The system also provides a summary of total number of licensees, number of overdue licensees, and percentage of overdue verifications.

Review Source History (UC32)

This use case enables a Licensing Agency to view and print a full history of an individual source's transfers and source status changes. This essentially provides a full life-cycle view of a source from cradle-to-grave.

Review Licensee's Inventory (UC33)

This use case enables a Licensing Agency to view and print a particular licensee's source inventory. The source information displayed includes: make/model, serial number, isotope, activity, activity unit, chemical form, physical form, device information, etc. Agencies can only view inventory of licensees in their respective jurisdictions.

Review Lost and Stolen Sources (UC34)

This use case enables a Licensing Agency to view and print a report of sources that have been reported as lost or stolen. The report will contain pertinent information including source make/model, serial number, source ID, possessing licensee's name, address, contact information, reporting date, comments, etc.

Review Long-term Storage Sources (UC35)

This use case enables a Licensing Agency to view and print a report of sources reported to be in long-term storage, that is, sources in the licensee's inventory that are no longer in use This information can be used to help DOE plan source recovery efforts.

Review Pending/Overdue Transfers (UC36)

This use case enables a Licensing Agency to view and print a report of pending or overdue transfers. A transfer is marked as 'Pending' if, during the 'Enter Unrecorded Sources' use case, the source is found to exist in another licensee's inventory. The other licensee must confirm or reject the transfer in order for the transfer to get out of the 'Pending' state. A transfer is marked

as 'Overdue' when the transfer has not been received within a set timeframe after the estimated arrival date. A Licensing Agency user will only be able to see transfers related to the licensees under the agency's jurisdiction

Review Import/Export Notifications (UC37)

This use case enables a Licensing Agency to search for and report on import and export notifications based on one or more criteria such as Notification Type (Import or Export), Date Range, Foreign Country, and Isotope. The information returned includes the US License Number, the foreign country, estimated departure date, originating address, ship-to address, isotope(s), etc.

Review Alert History (UC38)

This use case enables a Licensing Agency to search for and report on the detailed history of one or more alerts, including alert category, alert description, alert recipients, and alert status changes. A Licensing Agency user will only see alerts involving the agency's jurisdiction.

Query Sources (UC39)

This use case enables a Licensing Agency to search for and report on sources based on one or more criteria such as state, licensing agency, isotope, activity level, make and model, vicinity, license category, status (active, decayed, destroyed, irretrievable, lost or stolen, buried.) The user will be able to view, sort, and print the source information retrieved. A Licensing Agency user will only see sources possessed by the agency's licensees.

Query Licensees (UC40)

This use case enables a Licensing Agency to search for and report on licensees based on one or more criteria such as licensee name, license category, authorized isotopes, state, vicinity, and licensing agency, The user will be able to view, sort, and print the licensee information retrieved. A Licensing Agency staff can only query licensees under the agency's jurisdiction.

Query Transfers and Receipts (UC41)

This use case enables a Licensing Agency to search for and report on transfers based on one or more criteria such as shipment status, shipment type (domestic, import, export), date ranges for transfer or receipt, and characteristics of sending or receiving licensees—state, vicinity, licensing agency, and license category. The user will be able to view, sort, and print the source information retrieved. A Licensing Agency staff can only query transfers involving the agency's licensees.

Generate Ad Hoc Reports (UC42)

This use case enables a Licensing Agency to use a general purpose reporting tool (such as Crystal Reports) to create new or retrieve previously created ad hoc reports on data in the NSTS.

Verify Pending Make/Model (UC43)

This use case enables a Licensing Agency to review and verify the accuracy of a pending source make/model number entered by a user--typically a licensee. A pending make/model would have been entered when a make/model was not found (see use case "Enter Unrecorded Make/Model") during data entry in a source tracking transaction (for example, during entering "Manufacture a New Source"). The user will be able to search and select from among the pending make/model numbers, review the selected one, and approve or reject it. A pending

make/model cannot be rejected until all sources associated with the pending makes/models have been re-associated to appropriate makes/models.

Verify Pending Licensees (UC44)

This use case enables a Licensing Agency to review and verify the accuracy of a pending licensee entered by another user--typically a licensee. A pending licensee would have been entered when a licensee was not found (see use case "Enter Unrecorded Licensee") during data entry in a source tracking transaction (for example, during entering "Transfer Sources ".) The user will be able to search and select from among the pending licensees, review the selected one, and approve or reject it. A pending licensee cannot be rejected until all transactions involving this licensee have been resolved properly.

Verify Pending Locations (UC45)

This use case enables a Licensing Agency to review and verify the accuracy of a pending location entered by a user--typically a licensee. A pending location would have been entered when a location address was not found (see use case "Enter Unrecorded Locations") during data entry in a source tracking transaction (for example, during entering "Receive Sources "). The user will be able to search and select from among the pending locations, review the selected one, and approve or reject it. A pending location cannot be rejected until all sources associated with this location have been properly assigned to a valid location.

Update Alert Status (UC47)

Many of the alerts generated by business events require investigation and resolution. This use case enables a Licensing Agency to monitor and update the status of the alerts. The user will be able to search for, select, review, and update the status of alerts sent to him/her, or re-assign the alert to another user for action.

Record Import Consent/Notifications (UC60)

According to the IAEA Code of Conduct, exporting companies shall notify and/or obtain consent from the importing countries for Category 1 or Category 2 sources. This use case enables a Licensing Agency to record an Import Notification received from a foreign company and indicate consent authorization.

Record Export Notifications (UC61)

Prior to exporting a source, a U.S. licensee must send an export notification to the foreign country that will receive it. A copy of that export notification is also sent to the NRC. This use case enables a Licensing Agency to record an export notification sent by a U.S. company.

Record Licensee Transactions (UC62)

This use case enables a Licensing Agency to perform activities (e.g., source transfers) in the system on behalf of its licensees. It also enables a parent licensee (e.g., a Master Materials License/Licensee) to enter information for its associated licensees / permitees. The Agency Staff or parent licensee enters the NSTS transactions as a surrogate for the licensee.

3.2.3 System Administration Requirements

The System Administration functional area contains requirements that primarily support the System Administrator activities for administering user accounts, managing acceptable values for data entry, and setting system wide parameters/rules.

Maintain License Relationship (UC26)

This use case enables the NSTS Administrator to link multiple licenses, so that reports, research, and analyses can be performed for a group of associated licenses. The user will be able to search and select a license to designate as the "parent" license, and to search and select one or more licenses to be "child" licenses. The user will also be able to disassociate licenses that have previously been linked.

Maintain User Accounts (UC49)

This use case enables the NSTS Administrator to create or update user accounts. The NSTS Administrator will be able to set up new user accounts, assign user IDs, and assign user roles, which will dictate which functions and data a user can access. This use case also enables authorized system users to modify some of their own account information and preferences.

Maintain Code Tables (UC50)

This use case enables the NSTS Administrator to store and modify various NSTS specific values (codes) used for lookups, defaults, and validations. Examples of code tables include activity unit, chemical form, isotope, licensing agency, make/model, shipment status, source status, country code, state code, etc.

Maintain Licensing Agencies (UC51)

This use case enables the NSTS Administrator to create and modify information about licensing agencies, including the main address, and the contact information.

Maintain Vicinities (UC52)

This use case enables the NSTS Administrator to store and modify a "vicinity" by specifying a unique vicinity name and list of U.S zip codes. A Vicinity is simply a geographical area delineated by a set of zip codes. Vicinities are used as a way to report on licenses, source inventory, and source transfers by geographical area.

Maintain Alert Rules (UC53)

This use case enables the NSTS Administrator to store and modify rules governing the behavior of alerts, for example, the primary and secondary recipients of each type of alert, and how the alert can be closed – by an event (for example, an overdue transfer is received) or by the primary recipient of the alert.

Maintain Report Schedules (UC54)

This use case enables the NSTS Administrator to set up rules governing which reports are run automatically, how often they are run, which people will receive the report, emails of recipients, etc.

Download NSTS Information (UCI-2)

This use case enables the NSTS Administrator to extract data from the NSTS for loading into specialized software outside of NSTS for display or analysis. Examples include: mapping software to display source distribution graphically; Geographic Information Systems (GIS) to query the information in relation to geographic position or features; and, statistical analysis software to aid in doing trend analysis on transfers and receipts.

3.2.4 System Timer Requirements

The System Timer functional area contains requirements that primarily support the event or time-triggered processes, reporting, and external interface processing of the system.

Generate Alerts (UC46)

When certain events occur, the system generates an alert, presents it to the primary recipient on login to the system, emails it to designated alert recipients, and logs the alert in the system. Examples of generated Alerts for events include the following: reporting lost or stolen sources; reporting found sources; reporting an incomplete shipment; reporting a pending transfer being entered; reporting that a source has decayed below the Category 2 threshold, entering unrecorded sources; entering unrecorded make/models; entering unrecorded licensees; entering unrecorded locations; overdue transfer; and overdue inventory verification.

Display Current Alerts (UC48)

An authorized user will be able to see a list of the alerts currently open and assigned to that user. This alert list would be automatically presented to the user when he/she logs into the system. The system would present a convenient way to select and update an open alert using use case "Update Alert Status.

Identify Overdue Transfers (UC55)

On a regular basis, the system will automatically mark transfers as 'overdue' if they have not been recorded as received within a given timeframe after the expected due date. When a transfer is identified as 'overdue' the system also generates an alert which is delivered to the designated Agency Staff (see use case "Generate Alerts"). Timeframes for automatically marking a transfer as overdue and for generating an alert can be variably set in the system through the code tables (see use case "Maintain Code Tables").

Calculate Source Decay (UC56)

On a regular basis, the system will automatically calculate the current activity level for all the sources in NSTS that have not reached an end-point in the life-cycle. When the activity level falls below the Category 2 threshold, the system will mark that source as decayed out of tracking range. Decayed sources will remain in the licensee's inventory and be able to be retrieved. Source decay below the tracking threshold will generate an alert which is delivered to the Licensee that possesses the source.

Generate Verification List (UC57)

Licensees will be required to annually verify their physical inventory against the inventory that is recorded in NSTS. After the annual verification due date, the system will generate a list of licensees who are required to submit verifications but have not done so. This list is used to report on overdue inventory verifications.

Notify of Overdue Verifications (UC58)

Licensees will be required to annually verify their physical inventory against the inventory that is recorded in NSTS. After the annual verification due date, on a regular basis the system checks each licensee's verification records. If a licensee's verification is overdue, the system will generate an alert which is delivered to the licensee (see use case "Generate Alerts"). The interval and frequency of the alerts are maintained in the code tables (see use case "Maintain Code Tables").

Generate Scheduled Reports (UC59)

NRC, Agreement State, and DOE Staff, as well as various indirect users of NSTS (e.g., other agencies) need to receive NSTS information via reports that are periodically generated. The system will generate reports according to a schedule which is configured by the NSTS Administrator.

Upload NSTS Information (UCI-1)

The DOE, Licensing Agencies, and Licensees will be able to send the NSTS required information in electronic files that can be batch loaded into the system. The purpose of batch loading is to allow NSTS to accept data from another system and to eliminate the need to have data entered manually in both the users' system and in NSTS. Authorized users will be able to upload information equivalent to most of the online NSTS transactions, for example: Manufacture New Sources or Regenerate Sources. This upload of information will be the primary means for DOE to load information from their RSRT (Radiological Source Registry Tracking) system into NSTS.

3.3 Performance Requirements

The Performance Requirements define non-behavioral attributes of the system that cover overall system performance and robustness. This includes characteristics such as workloads, response time, data integrity, data capacity, reliability, maintainability, and expandability.

3.3.1 External Workloads

The system must provide the capability to perform a batch load of license data on a periodic basis from the Web-based Licensing system and from other external systems including the Radiological Source Registry Tracking (RSRT) system of the Department of Energy (DOE). This would be used for the data load and for subsequent testing loads. The number of license records uploaded during a load will not exceed the total license count which is expected to be 20,000.

The system shall also provide the capability to perform a batch extract and export of all NSTS data on an as needed basis. This would be used for providing licensee and source tracking information to other authorized federal agencies, for example, the Department of Homeland Security (DHS). The number of records downloaded upon request, will be equivalent to the total number of records in the system, including historical records.

3.3.2 Throughput, Response Times, and Internal Function Workload

- The system must provide acceptable response times for all functions of the system. In particular: the system must present screens to the user within 5 seconds of the user request; the system must complete sort operations within 5 seconds of the sort and save request; the system must save data to the database within 5 seconds of the save request; the system must display the results of a search operation within 30 seconds of the search request; and the system must present the user with a measurable indication of progress if there is more than a 10 second processing delay. The system must comply with these performance requirements while supporting the potential transactional load imposed by 20,000 licenses.

3.3.3 Data Quality, Integrity, and Accuracy

The system must fully utilize the data integrity, logging, and transaction management capabilities available in the Oracle database software to ensure data integrity. This includes referential integrity features (e.g., primary key / foreign key relationship constraints) and logical unit-of-work features (e.g., atomic rollback or commit). The system must also provide the ability to generate a unique identifier for a record created in the system. Through system and database constraints, the Contractor shall ensure that the generated identifier may not be altered by any user at any time.

The system must provide the capability to maintain a history of data changes to facilitate auditing activities. This includes automatically recording the date/time, the data changed, and the user that changed the data as part of the history record. This also includes providing the NRC with the ability to specify which tables and associated data elements should be audited and what types of changes should cause a history record to be created (e.g., insert, update, and delete). The historical data must be formatted in a way that facilitates the simple visual comparison of current data to historical data. The ability to configure or view audit records will be restricted by user role.

3.3.4 Data Retention, System Capacity, and Communications Capacity

The operational system must retain all operational and historical data for the life of the system. The system must provide the system capacity to support 20,000 licenses. Additional storage space will be added to the system as needed to meet growth requirements. The system must provide a minimum of 3 megabit/second network bandwidth for NRC users of the system. There will be 20,273 user accounts with up to 400 simultaneous Web users. Note: The data retention, system capacity, and communications capacity requirements are for the Operational/Production environment only; the Contractor can propose a development environment suitable for software development and testing purposes.

3.3.5 Reliability, Maintainability, and Availability

The operational system must be available 99.9% of the time 24 hours a day / 7 days a week except during regularly scheduled maintenance. Regularly scheduled maintenance must not be performed during the core business hours of 6AM to 10PM EST Monday through Friday and must not last for more than 3 hours in any 24 hour period without a waiver from the government. The contractor shall notify the NRC in advance of any regularly scheduled maintenance. The system must employ an architecture that utilizes multiple types of redundancy to ensure automatic failover (e.g., hardware component redundancy, server clusters, data mirroring, load balancing, uninterruptible power supplies, etc). The system must provide the ability to monitor for software and hardware component failures and be able to automatically transition to a redundant system or set of sub-components within 30 minutes.

3.3.6 Growth, Flexibility, and Expandability

The system must provide a scalable architecture that allows system resources to be easily added as needed. This includes providing the ability to share the system processing duties across clusters of servers in order to provide load balancing and high availability advanced features. This also includes providing 'hot-swap' features that enable easy replacement or

upgrade of entire system servers or their hardware sub-components without interrupting overall system operation.

The system must provide an easily extensible modular architecture that facilitates the enhancement of the system via properly encapsulated custom modules that are only loosely coupled to the main system. The system must support upgrades to the software that are not affected by custom modules and do not lose any previously entered system configuration information. This system must also provide a published application programming interface (API) to allow other systems to access information programmatically. The system must consist of highly scalable software components designed for high performance, high concurrency, and low system resource footprints.

The system must provide the capability for the NRC to dynamically create and enforce custom business rules. This includes: data entry rules used to specify data elements that are required, have default values, use code lookups, follow particular formatting rules, and/or are subject to specific validation rules; and processing rules used to specify special calculations or formulas; code tables used to add, modify, and delete entries in the various application code lookup tables; and scheduled actions used to dynamically schedule system batch jobs (e.g., imports, exports, etc).

3.3.7 Backup and Recovery

The system must provide robust backup and recovery capabilities. This includes performing an online backup without requiring system down time, storing backups at an off-site storage facility, and restoring from a full backup within one hour. The system must provide the ability to perform full and incremental backups on a scheduled basis as defined by the system administrator. Full backups will be performed at least weekly and incremental backups will be performed at least daily.

3.4 Operational Requirements

The Operational Requirements define non-behavioral attributes of the system that cover the operational environment of the system. This includes characteristics such as human interaction guidelines, physical environment standards, configuration control practices, security needs, and documentation deliverables.

3.4.1 Human Factors

The system must conform to industry standard conventions for common usability. This includes the IBM published Common User Access advanced interface design standards, the Microsoft published Windows interface design standards, the Section 508 standards of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, as it applies to internet web applications and client / server applications, and NRC Management Directive 3.14, concerning external web site standards (attached in Appendix C). Of particular importance, are the areas of consistency, visual cues, navigational assistance, user preferences, and standard productivity features.

The system must provide a high degree of user interface consistency with regard to screen layouts, graphics, reserved words, text font and styles, text meanings, and navigational

metaphors. Note: The system must follow the Unicode standard so that it can support non-English alphabets (e.g., used for make, model, and serial number values).

The system must provide visual cues to help the user interact with the system. Some examples include: an hourglass for a short wait, a 'progress box' for a long wait, a warning message prior to a destructive action, an error message if an error occurs, etc. The system must not use color as the only way of conveying information.

The system must provide simple methods for navigating through the application's functions. This includes: providing a quick way to access frequently used or essential tasks (i.e., accelerator keys or key combinations); providing complete and equal access to all application functions from both the mouse and the keyboard; and providing a mechanism for indicating the user's position within the system (i.e., a traceable path).

The system must enable the user to adapt the application to his/her work patterns via user-defined application preferences (e.g., functional options, toolbar placement, color choices, etc).

The system must provide the user with standard productivity features. This includes providing: sophisticated dynamic sort functionality (e.g., single-field sort, multi-field sort, visual sort display); wild-card search functionality; standard print functionality; standard save to file functionality; and email interaction functionality.

3.4.2 Facilities, Environment, Safety, System Monitoring, and Support Capabilities

The system must be hosted in an appropriate computer data center environment. The servers must be maintained in a properly climate-controlled facility that meets all appropriate safety standards for a data center and there must be sufficient production control support staff available to proactively monitor the system for potential problems and bottlenecks.

The system must support the following server, client, and web platforms. The server platform must employ the LINUX operating system. The client platform must be the standard NRC desktop environment in effect at the time of deployment (currently Windows XP). The web portion of the system must support, at a minimum, version 5.0 or greater of both Microsoft Internet Explorer and Netscape Navigator web browsers.

The system must support access from Crystal Reports and MS Access tools for ad-hoc reporting (e.g., via data extraction).

3.4.3 Configuration Control

The production system must employ formal change management and version control practices via automated configuration control software (Rational ClearCase).

3.4.4 Security

The security classification for this system has been determined to be 'Sensitive Unclassified--Official Use Only' (also known as 'OUO'). There will be no privacy data required or retained by the system. Following the guidance of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 *Guide for Mapping Types of Information and Information*

Systems to Security Categories, an analysis of the sensitivity of NSTS information determined the sensitivity to be "high" which will require the system to have appropriate security controls to protect the confidentiality, integrity and availability of the data. Such security controls shall meet the assurance requirements and protective measures specified in NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, for a system with "high" sensitivity of information.

In keeping with the best practices in federal agencies and the private sector to protect highly sensitive information, the system implementation shall include digital certification functionality to ensure that only authorized users of the system have access to it. NRC and Agreement State licensees will be required to obtain digital certification under NRC procedures in order to use the NSTS. The system shall provide the capability to securely accept user security credentials that have been authenticated by an external authentication system (e.g., a Lightweight Directory Access Protocol (LDAP) repository, an Oracle SSO server, etc.). This authentication system will be provided by the NRC. NIST SP 800-63 *Electronic Authentication Guideline*, shall be used to guide implementation of authentication controls. For a system requiring "high" controls, level 4 is appropriate.

The system shall provide the capability to support role driven permissions for determining access to objects (e.g., menu options, screens, specific functions, data groupings by region, etc.) in the system; as well as record types sent in an upload file that are acceptable by the system. The system shall provide the capability to perform audit tracking on modifications to the security permissions for users and roles.

The system shall provide the System Administrator with the capability to configure the password requirements for all users. This includes characteristics such as minimum length, formatting rules, expiration dates, and encryption.

The system shall provide the ability to encrypt data in transit according to Federal Information Processing Standards Publication (FIPS PUB) 140-2 to prevent eavesdropping. While FIPS PUB 140-2 supercedes FIPS PUB 140-1, products that were validated to 140-1 are still valid. New products must be validated to 140-2. The system shall have the ability to encrypt non-public data for transmission over various media, locally and remotely. Encryption shall be assignable based on the contents of the record. The system shall provide the System Administrator the ability to designate what algorithm should be used to encrypt data for transmission. Any encryption required in this system shall use the FIPS approved MODE of products and algorithms validated to FIPS PUB 140-1 or 140-2 (algorithms must be FIPS PUB 140 validated as shown on the product's FIPS 140 certificate.)

3.4.5 Documentation

The system must include a full set of electronic and hard-copy documentation that describes all aspects of the system. This includes: user documentation to assist the user with completion of all application functional tasks; deployment documentation that describes system deployment activities; administrative documentation for the technical staff that describes system administration and configuration; security documentation that describes the security aspects and controls of the system; and training documentation to assist with the training of the new users of the system.

3.5 Programmatic Requirements

The Programmatic Requirements define non-behavioral attributes of the system that cover the other system environments needed for development and testing activities.

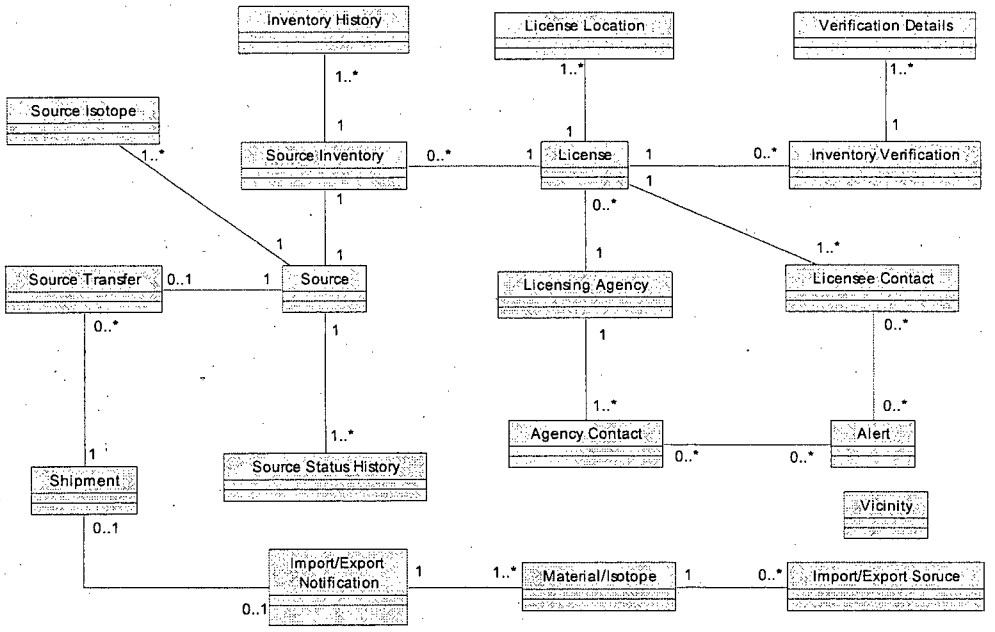
3.5.1 Development Facilities and Support Requirements or Constraints

The system must include a development and test environment that is comparable to the production server environment and is supported by system personnel during routine business hours of the development contractor and any partners that may be dependent upon this environment.

3.6 Data Requirements

The Data Requirements define the top-level data entities and their relationships. Exhibit 3-3 is a graphical representation of the top-level data entities. Additional details about each entity are provided in Appendix B: SafeSource Phase II Requirements Analysis.

Exhibit 3-3: Business Object Model



- Attributes do not include fields needed for audit purpose.
- Logical Model does not reflect necessary table normalization.

Notation:

A —1— B	An *A* is always associated with one *B*.
A —1..*— B	An *A* is always associated one or more *B*.
A —0..1— B	An *A* is associated with zero or one *B*.
A —0..*— B	An *A* is associated with zero, one or more *B*.

4. WBL SYSTEM REQUIREMENTS – OPERATIONAL SUPPORT AND MAINTENANCE

SafeSource Phase I Web-based Licensing (WBL) is undergoing system development and deployment under a separate SafeSource Phase I contract. The SafeSource Phase II contract, however, includes transferring WBL to the SafeSource Phase II Application Service Provider (ASP) and supporting the ongoing operations of WBL along with NSTS beginning per the NRC accepted schedule for Task 3.1. This section describes the operational aspects of the system and not the functional aspects. The Contractor shall meet all WBL requirements for operations and maintenance.

4.1 Overview

This section provides a high-level description of WBL in terms of its overall system concept, its operational architecture, and its interfaces with external systems.

System Concept

WBL streamlines the materials licensing process for licensees and NRC staff; it also supports related activities including inspections and reciprocity arrangements between the NRC and Agreement State licensees. Major functions of the WBL system include the following:

- New applicants and existing NRC licensees will be able to establish a Web-based user account to submit and track requests to apply for, amend, renew, or terminate licenses to manufacture, distribute, and use nuclear materials in NRC-jurisdiction states for commercial purposes.

- Existing nuclear materials licensees from Agreement States (states which are delegated authority by the NRC to issue such licenses in their jurisdictions) will be able to establish a Web-based user account to submit and track requests to apply for, amend, or renew temporary ("reciprocity") licenses to manufacture, distribute, and use nuclear materials in NRC-jurisdiction states for commercial purposes.

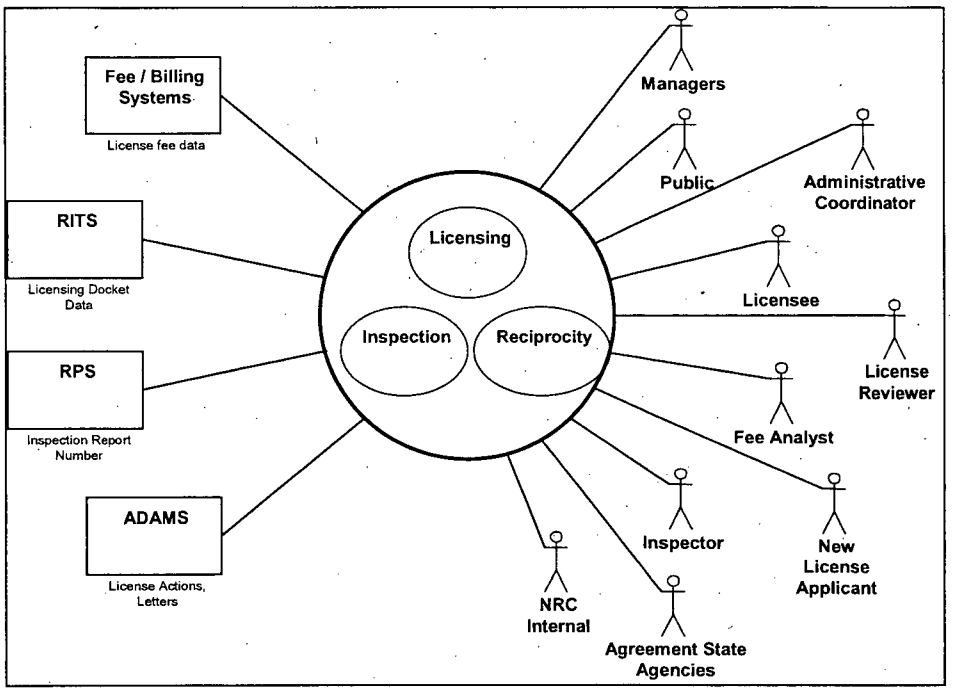
- NRC managers and licensing staff will use the system to organize and track their work reviewing and approving licensing requests, including communication with new applicants and existing NRC licensees and issuance of new and amended licenses.

- NRC managers and inspection staff will use the system to organize and track their work scheduling, preparing, executing, and following up on inspections of nuclear materials licensees and their facilities.

- Various classes of users, including the public, will have selective access to these functions and to the information captured in the database. The system will produce various standard queries, reports and interfaces to existing NRC systems as well as allow ad hoc query and reporting.

Exhibit 4-1 shows the major classes of users and the system interfaces that form the context for the SafeSource Phase I system.

Exhibit 4-1: SafeSource Phase I WBL System Context



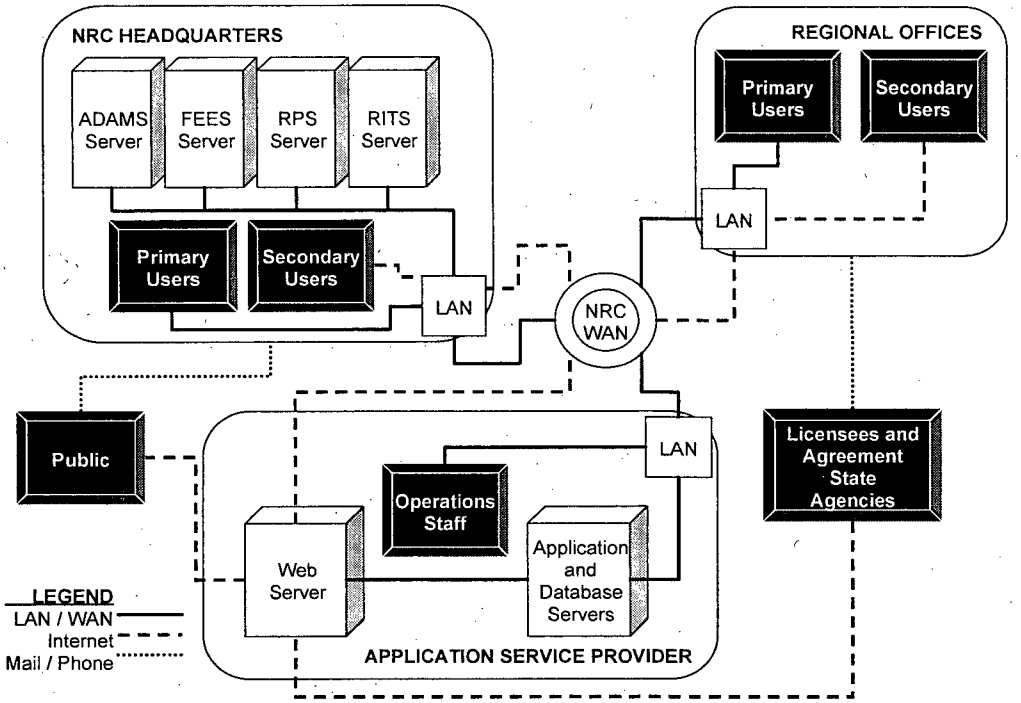
The Context Diagram (Exhibit 4-1) shows direct users of WBL (shown as stick figures) and automated systems (shown as rectangles) that will interface with WBL. The system provides a web-based platform that can be accessed by licensees, public, Agreement State agencies, and NRC. The WBL program and support staff can access WBL via LAN or WAN, which include Administrative coordinator, Fee Analyst, Inspector, License Reviewer, Manager that are located in both headquarters and regional offices. The Licensees, New License Applicants, Agreement State agency staff, Public, and other NRC Internal users can access WBL via the Web.

WBL interfaces with several existing NRC systems by providing needed information. These systems include the Agencywide Documents Access and Management System (ADAMS), Material Annual Fee System (MATANN), Material Fee Billing System (MATFB), License Fee Reporting System (FEES), Regulatory Information Tracking System (RITS), and Reactor Programs System (RPS).

Operational Architecture

The WBL is a secure web-based application. WBL is developed using an Oracle based Commercial Off-The-Shelf (COTS) licensing package from Versa Systems called LicenseEase. The system will be operated by the same Application Service Provider that operates the NSTS. The operational architecture is depicted in Exhibit 4-2.

Exhibit 4-2 SafeSource Phase I (WBL) Operational Architecture



NRC users at Headquarters and in Regional Offices will access the system using LAN and WAN connectivity. External users including licensees, Agreement State agencies, and the public will be able to access the system if desired using their local Internet connectivity. The NRC will continue to provide support to any external users who chose to interact via telephone or by mailing paper-based transactions.

The core SafeSource Phase I user community will encompass approximately 158 NRC specific internal individuals ("named users") with read-write capability:

- Administrative Coordinators--17
- License Reviewers--58
- Inspectors--41
- Managers--22
- Fee Analysts--5
- IT Support Staff --15

The breakdown of these users by location is shown in the Exhibit 4-3.

Exhibit 4-3: SafeSource I WBL Users by Type and Location

User Type	Region I	R-I/R-II Atlanta	Region III	Region IV	HQ	Total
Administrative Coordinators	4	1	4	1	7	**17**
License Reviewers	20	0	15	13	10	**58**
Inspectors	7	11	14	6	3	**41**
Managers	4	2	3	3	10	**22**
Fee Analysts					5	**5**
IT Support Staff					15	**15**
Total	**35**	**14**	**36**	**23**	**50**	**158**

External users including Licensees, Agreement State Agencies, and the Public will be able to access the system if desired using their local Internet connectivity or connectivity provided by the ASP. NRC Internal users also will access the system via the NRC Internet connectivity. Internet-based access will include:

- NRC Internal users
- Public–limited read-only access
- Licensees–limited read-write access

The system will provide support for 558 named user accounts – 158 internal users and 400 simultaneous web users.

System Interfaces

Batch extraction interfaces are established between the SafeSource Phase I WBL system and the following existing NRC systems that are operated in the NRC internal computing environment:

- Agencywide Documents Access and Management System (ADAMS) – For NRC Archival, certain WBL generated output and information are sent to ADAMS in Adobe Portable Document Format (PDF) format along with a suggested set of meta-data information used to properly categorize the submission within ADAMS.

- Various NRC Fee Systems – Periodically, WBL generates and exports the necessary file (with basic docket and licensing information and a list of fee categories that apply to a given license) needed by various NRC fee-related systems according to a NRC-configurable schedule:
  - Material Annual Fee System (MATANN)
  - Material Fee Billing System (MATFB)
  - License Fee Reporting System (FEES)

- Regulatory Information Tracking System (RITS) – WBL generates and exports the necessary file (with basic docket and licensing information and a list of fee categories that apply to a given license) needed by the Regulatory Information Tracking System (RITS) according to a NRC-configurable schedule.

- Reactor Programs System (RPS) – WBL generates and exports the necessary file containing basic inspection data needed by the Reactor Programs System (RPS)

according to a NRC-configurable schedule.

4.2 Functional Requirements

The functional requirements of WBL are included in a separate SafeSource Phase I contract for system development and deployment. Therefore, the functional requirements are not included in this document.

4.3 Performance Requirements

The performance requirements of WBL are the same as NSTS as described in section 3.3.

4.4 Operational Requirements

The operational requirements of WBL are the same as the NSTS as described in section 3.4.

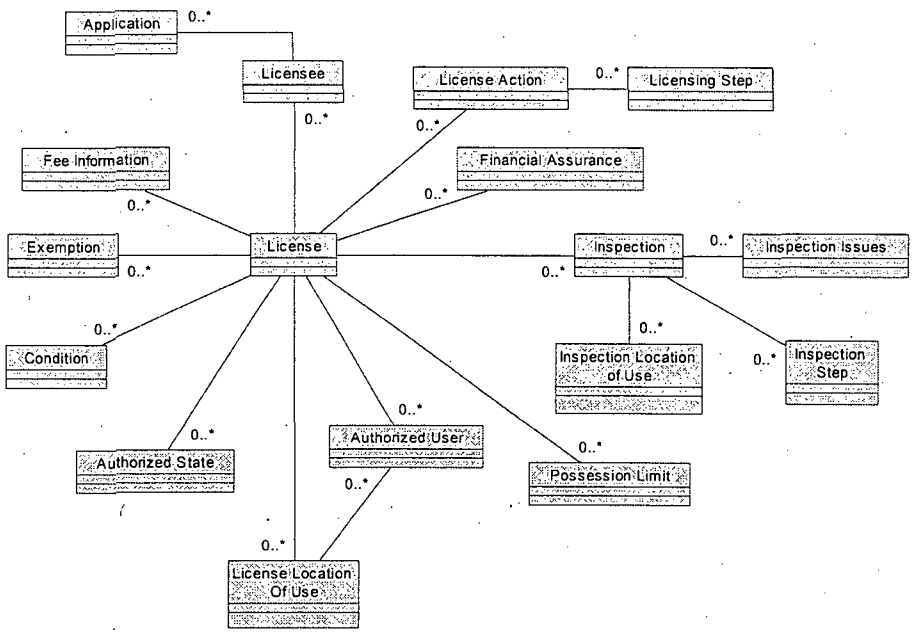
4.5 Programmatic Requirements

The programmatic requirements of WBL are the same as NSTS as described in section 3.5.

4.6 Data Requirements

Exhibit 4-4 is a graphical representation of the top-level data entities of WBL.

Exhibit 4-4: WBL Business Object Model



Notation:

A —1— B	An ***A*** is always associated with one ***B***.
A —1..*— B	An ***A*** is always associated one or more ***B***.
A —0..1— B	An ***A*** is associated with zero or one ***B***.
A —0..*— B	An ***A*** is associated with zero, one or more ***B***.

5. CONTRACTOR PERFORMANCE REQUIREMENTS

5.1 Overview

The Contractor shall perform the one development task, provide at least one year of operational support, maintenance, and user support, and perform a second development task should NRC execute this option. This section describes each of the tasks in this contract:

- Task 1: Establish Initial NSTS (Release 1/NSTS V1)
- Optional Task 2: Develop Enhanced NSTS (Release 2/NSTS V2)
- Task 3: Operational Support
- Task 4: Maintenance
- Task 5: User Support

Exhibits 5-1 and 5-2 on the following pages show a breakout of the NSTS use cases (functional requirements) that will be implemented in Tasks 1 and 2. Use cases are summarized in Section 3 of this PBSOW and detailed in Appendix B, SafeSource Phase II Requirements Analysis.

Exhibit 5-1: Breakout of Licensee Functions by NSTS Development Release

Use Cases (Functions)	Release 1	Release 2
Record Source Starting Points		
1. Manufacture New Sources	✓	
2. Regenerate Sources	✓	
Transfer Sources		
3. View Transfer Progress		✓
4. Transfer Sources (domestic)	✓	
5. Export Sources	✓	✓[4]
6. Update/Cancel Source Transfers	✓	
7. Verify Pending Transfers	✓	✓[4]
8. Review Licensee Transfer History		✓
Receive Sources		
9. Receive Sources (domestic)	✓	✓[4]
10. Receive Imports	✓	✓[4]
Manage Source Inventory		
11. Record Source Location	✓	
12. View Own Inventory	✓	
13. Verify Source Inventory		✓
14. Specify Long-Term Storage Sources		✓
15. Update Source Information	✓	
Unrecorded Information		
16. Enter Unrecorded Sources	✓	✓[4]
17. Enter Unrecorded Transfers	✓	✓[4]
18. Enter Unrecorded Locations	✓	✓[4]
19. Enter Unrecorded Make/Model	✓	✓[4]
20. Enter Unrecorded Licensees	✓	✓[4]
Record Source End Points		
21. Dispose of Sources	✓	
27. Record Destroyed Sources	✓	
User Support		
22. Obtain Supporting Information		✓
23. Send Message to NSTS Mailbox		✓

[4] Part of the functionality of this use case is contained in Release 1, part in Release 2. See Appendix B for details.

Exhibit 5-2: Breakout of Agency/System Functions by NSTS Development Release

Use Cases (Functions)	Release 1	Release 2
Manage Licensee Information		
24. Create Licensees	✓	✓[5]
25. Update/Delete Licensee Information	✓	
26. Maintain License Relationship		✓
Record Source Incidents		
28. Record Lost or Stolen Sources		✓
29. Record Found Sources		✓
30. Record Irretrievable Sources		✓
Generate Queries		
31. Review Inventory Verifications		✓
32. Review Source History		✓
33. Review Licensee's Inventory	✓	
34. Review Lost and Stolen Sources		✓
35. Review Long-Term Storage Sources		✓
36. Review Pending/Overdue Transfers		✓
37. Review Import/Export Notifications		✓
38. Review Alert History		✓
39. Query Sources		✓
40. Query Licensees		✓
41. Query Transfers and Receipts		✓
42. Generate Ad Hoc Reports		✓
Alerts & Verifications		
43. Verify Pending Make/Model	✓	✓[5]
44. Verify Pending Licensees	✓	✓[5]
45. Verify Pending Locations	✓	✓[5]
46. Generate Alerts		✓
47. Update Alert Status		✓
48. Display Current Alerts		✓

[5] Part of the functionality of this use case is contained in Release 1, part in Release 2. See Appendix B for details.

Exhibit 5-2: Breakout of Agency/System Functions by NSTS Development Release (continued)

Use Cases (Functions)	Release 1	Release 2
Administer NSTS		
49. Maintain User Accounts	✓	
50. Maintain Code Table	✓	✓[6]
51. Maintain Licensing Agencies	✓	
52. Maintain Vicinities		✓
53. Maintain Alert Rules		✓
54. Maintain Report Schedules		✓
55. Identify Overdue Transfers		✓
56. Calculate Source Decay		✓
57. Generate Overdue Verification List		✓
58. Notify of Overdue Verifications		✓
59. Generate Scheduled Reports		✓
62. Record Licensee Transactions	✓	✓[6]
Import/Export		
60. Record Import Consent and Notification		✓
61. Record Export Notification		✓
System Interfaces		
I-1. Upload NSTS Information	✓	✓[6]
I-2. Download NSTS Information		✓

[6] Part of the functionality of this use case is contained in Release 1, part in Release 2. See Appendix B for details.

5.2 Methodology Compliance

The NRC requires that all Contractors who are either developing or maintaining NRC information systems comply with the prevailing agency methodology and procedural requirements for such efforts. The NRC is in the process of implementing a new Project Management Methodology (PMM) for software development projects. This methodology replaces the previous NRC System Development Life Cycle Management Methodology. The NRC PMM is based on the Rational Unified Process (RUP), augmented to address broader issues of federal IT projects. PMM artifacts are drawn from RUP, with tailoring to better fit the NRC context. Of main concern to the Contractor are the products and artifacts that they must provide for compliance with the PMM. In addition to the PMM, the Contractor shall also comply with supplementary NMSS standards such as those governing design modeling and automated software testing.

For all written deliverables, models, diagrams, and graphics, the Contractor shall deliver a draft for NRC review and shall deliver further versions until all concerns are addressed to the satisfaction of the NRC Project Manager. All deliverables of this nature shall be delivered to the NRC in both hard copy and electronic form as specified in Section 7.1.

The Contractor shall ensure that all activities are conducted and all products delivered in accordance with the NRC Project Management Methodology (PMM) processes as defined on the NRC internal web site as of July 24, 2007.

5.3 Task 1: Establish Initial NSTS

Scope of Work

The initial system will implement Release 1 of the NSTS (V1):

This version will provide the basic Web-based functionality needed to meet the new NRC source tracking regulations and the IAEA Code of Conduct requirements for source registry. It will be accessible to limited NRC, DOE, and Agreement State (A/S) personnel, and will be deployed to affected nuclear materials licensees (and appropriate DOE facilities) in two phases. Each deployment group will comprise a "supply chain" of manufacturer/distributors, source users, and disposers, so that sources can be tracked through their life-cycles within that group.

Task 1 includes support for public workshops to familiarize affected licensees with use of the NSTS.

Schedule and Detailed Task Descriptions

The Task 1 schedule is presented in Appendix D and is reflected in the Exhibit 5-3 deliverable schedule. Detailed task descriptions are provided below.

Performance of the detailed tasks by the Contractor is non-negotiable. However, the Contractor may propose different task durations and to some extent revised task sequencing within the iterative PMM template context represented in Appendix D and Exhibit 5-3. In doing so, the Contractor shall maintain the key NRC milestones and meet all performance requirements described in Appendix A. In proposing a technical approach, the Contractor shall conform to the

"Design and Implementation Controls" identified in Section 6. The Contractor is encouraged to propose a schedule that optimizes use of Contractor resources to provide for an earlier deployment date. In doing so, the Contractor shall not compress schedule intervals proposed for reviews and other activities to be conducted by personnel from the NRC, IV&V contractor or other agencies.

Task 1.1 Obtain Development Environment Purchase Approval

The Contractor shall prepare and deliver for NRC approval procurement packages for all software products, infrastructure products (servers, and telecommunication services or lines), and hosting services that were identified in the contract proposal. Although Task 2 is optional and may not be pursued, the Contractor shall prepare and deliver procurement packages for all development environment elements needed for Tasks 1 and 2. The Contractor shall prepare a separate procurement package for each proposed vendor order. In each package, the Contractor shall present three competitive quotations from GSA schedule vendors and justify any recommendation to use other than the lowest cost vendor.

Task 1.2 Develop Software Development Plan (SDP)

The Contractor shall develop and deliver to the NRC a Software Development Plan, using the prevailing PMM template. The current SDP template is attached in Appendix E. The SDP is in effect the project management plan from the Contractor's perspective. In this plan, the Contractor shall expand upon the basic plan submitted in the Contractor's written portion of the proposal. In particular, the Contractor shall highlight in the SDP any significant changes or deviations from the technical approach described in the contract proposal, citing the NRC approval of each change or deviation. The Contractor shall include in the SDP any proposal for delivery of interim system builds to expedite NRC review and provide timely compliance feedback.

While all SDP content is required, the NRC has several areas of particular concern. To address these, the Contractor shall address, in Section 4.2 of the SDP, how it will manage the project to minimize disruptions in NRC business activities. In SDP Sections 4.2.5.1 and 4.5 (Risk Management Plan), the Contractor shall further describe the approach to retain key staff, and address potential technical or schedule issues.

Task 1.3 Develop Quality Assurance Plan (QAP)

The Contractor shall develop and deliver to the NRC a comprehensive Quality Assurance Plan (QAP), using the prevailing PMM template. The current QAP template is attached in Appendix F.

Task 1.4 Install Development Environment

Following NRC approval under Task 1.1, the Contractor shall purchase, install, and set up the NRC-approved development environment at the Contractor's site or another approved location so that system development activities can commence. As part of the setup activity, the Contractor shall perform any NRC-specific software configuration needed, as well as establishing connectivity and preparing the servers (e.g., hardening) to meet the external hosting requirements.

The Contractor shall host all NSTS server hardening activities at Contractor facilities. The Contractor shall provide support as required in NRC development of hardening guidance related to software or hardware technologies to be utilized in the NSTS architecture. The Contractor shall harden all NSTS architecture components to meet NRC standards and shall support all

independent NRC hardening verification reviews. The Contractor shall conduct ongoing hardening activities related to timely application of software patches. The Contractor shall conduct monthly hardening verification scans and provide to the NRC scan results and reports summarizing issues identified and resolution status for each issue.

Task 1.5 Validate Requirements

The Contractor shall conduct an effort to validate the NSTS Task 1 requirements. In this effort, the Contractor shall hold workshops, conduct interviews, and otherwise obtain requirement specification concurrence from representatives of all stakeholder groups. The foundation for this effort is Appendix B, SafeSource Phase II Requirements Analysis. Following requirements validation, the Contractor shall submit to the NRC proposed revisions to requirements documentation, in particular the baseline use cases. The Contractor shall also deliver to the NRC a report summarizing the findings of the validation effort. The Contractor shall submit proposed revisions to requirements in the form of marked-up Use Case documents. The Contractor shall export all Use Cases requiring revision from the NSTS RequisitePro repository. Following revision, the Contractor shall place the revised Use Cases in a shared storage location pending NRC review.

Task 1.6 Develop Deployment Plan

The Contractor shall develop and deliver to the NRC an overall deployment plan, compliant with the PMM template found in Appendix G. Although optional Task 2 may not be pursued, within the SDP, the Contractor shall describe the approach addressing the complexities of possibly working concurrently on Task 1 and Task 2.

In the Deployment Plan, the Contractor shall also identify the steps and procedures which the Contractor will employ to deploy the NSTS to NRC users, including plans for training, and to support three groups of licensees as they start using the system in succession. The Deployment Plan shall address any issues regarding labor and other resources, timing, sequence and schedules, and any other contingencies.

Task 1.7 Develop Configuration Management Plan (CMP)

The Contractor shall develop a Configuration Management Plan (CMP). In this plan, the Contractor shall propose the necessary NRC-funded hardware and software to host a Rational ClearCase CM server at the Contractor development site. The Contractor shall propose and provide costs for Configuration Management (CM) coordination with the NRC central CM repository system. The Contractor shall propose an approach for periodically transmitting project artifacts to the NRC CM repository, as directed by the NRC.

In CM and other affected proposal areas, the Contractor shall address the NRC intent to provide periodic IV&V oversight throughout the requirement validation, design, development, and testing processes. For this reason, the Contractor shall plan for an environment that facilitates inspection of program code and other project artifacts by the IV&V team from NRC headquarters.

Task 1.8 Develop Detailed Design

The Contractor shall develop and document the detailed NSTS design using UML models, supporting reports, and a Supplemental Design Document. In developing design models and documentation, the Contractor shall comply with specifications found in Appendix I, Detailed Design Standards. Although Task 2 is optional and may not be pursued, the Contractor shall include in the Task 1 detailed design high-level references for Task 2 functions.

Task 1.9 Develop Software Architecture Document (SAD)
In the NRC PMM, the SAD is used to express all aspects of the logical and physical system design at a high level, mainly for use by NRC enterprise architects. In an extension to the general requirement for draft and final versions of Contractor document deliverables, for the SAD, the Contractor shall deliver products representing an initial design, following requirements validation, and a final design prior to proceeding with system development. In both iterations, the Contractor shall accommodate NRC review and provide revised products addressing NRC concerns. The Contractor shall also repeat the cycle of revision and NRC review should the design change prior to NRC acceptance of Task 1 software for production deployment. In developing the SAD, the Contractor shall use the PMM template attached in Appendix H. It is notable that the Contractor shall begin with the NRC-provided SAD V1.0, reflecting preliminary design information. This will result in the first Contractor SAD deliverable being V1.1.

Task 1.10 Conduct Design Review
The Contractor shall develop and deliver a comprehensive design review presentation for NRC's senior management and SafeSource stakeholders that covers the entire system capability, including those requirements to be implemented in Tasks 1 and 2. References to Task 2 functionality will be at a high level. At NRC direction, the Contractor shall expend up to 300 labor hours preparing animated mock-ups of key system functions and present these during the review.

Task 1.11 Develop System
The Contractor shall construct system components that are needed to implement required Task 1 system functionality in accordance with the approved system design and validated requirements. In accordance with the NRC Project Management Methodology (PMM), the contractor shall deliver for NRC inspection interim builds, reflecting iterative inclusion of NSTS Release 1 content.

Should the Contractor propose a commercial off-the-shelf (COTS) product as part of the solution, the Contractor shall comply with the NMSS COTS Policy document in Appendix J. Furthermore, if both custom sub-systems and a COTS product are employed in the solution, the Contractor shall construct custom sub-systems in a way that does not interfere with the ability to deploy subsequent COTS version upgrades. This task relates to compliance with one or more contract performance requirements reflected in Appendix A.

The Contractor shall isolate development of NSTS V1 software components affected by security access controls. To enable optimal schedule compression and development progress during security architecture analyses, the Contractor shall only pursue development of software modules not directly affected by security access controls.

Task 1.12 Conduct Data Conversion
The Contractor shall organize, transform, package (or otherwise pre-format), and migrate structured and unstructured data to establish the fully-functional database of historical and active records using the agency's existing data sources (e.g., the Interim Source Database, WBL, and National Sealed Source & Device Registry System) as input.

The main source of data for the initial NSTS database load will be the Interim Source Database (ISD). The NRC solicits updates to this database from 25% of the affected licensees each quarter. Given this, data currency will be an issue during the months of NRC acceptance testing and phased STS deployment to the NRC users and three licensee groups. It is also notable that some licensee data is collapsed to the licensee level in the ISD, not providing

details on individual sources. If available, these source-level details must be provided in the NSTS data refreshes performed prior to each licensee group roll-out. The NRC expects to implement new regulations by the end of 2006, requiring reporting at the source level.

The Contractor shall build the initial NSTS database using other sources and an ISD snapshot captured at a time deemed acceptable by the NRC. This initial NSTS database will be used for NRC NSTS V1 acceptance testing and for licensee workshop demonstrations.

The Contractor shall use the latest data available from the ISD and other sources, and refresh the NSTS database as close as possible to the time of NSTS deployment to each of the three licensee groups. This will result in the initial NSTS database and three subsequent updated versions prior to full NSTS V1 production deployment.

This Contractor shall document and test the initial data conversion activity and subsequent updates to ensure that all data elements and records are retrieved, integrated, and accurately reflected in the NSTS database. The Contractor shall provide data conversion design plans, data conversion scripts, post-conversion comparison reports and test result artifacts to the NRC, in support of IV&V processes.

This task relates to compliance with a contract performance requirement reflected in Appendix A.

Task 1.13 Perform System Security Risk Assessment

The Contractor shall perform a risk assessment of the NSTS and shall develop a strategy to address all identified NSTS security risks. The assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation and are required by the Federal Information System Management Act (FISMA) and OMB Circular A-130, Appendix III. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans. The risk assessment shall characterize the information processed by the NSTS using Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories.* The risk assessment shall follow NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, and include the following:

- Identification of NSTS user types and associated roles and responsibilities
- Identification of risk assessment team members and their associations
- A description of the risk assessment approach and techniques, where the techniques include documentation review, interviews, observation, and hands-on system assessment
- A description of the risk scale used, including at a minimum, the potential impact as defined in FIPS 199, and likelihood as defined in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- A list of potential system vulnerabilities

- A list of potential threat-sources applicable to the system, including natural, human, and environmental threat-sources
- A table of vulnerability and threat-source pairs and observations about each
- Detailed findings for each vulnerability and threat-source pair discussing the possible outcome if the pair is exploited; existing controls to mitigate the pair; the likelihood determination as high, moderate, or low; the impact determination expressed as high, moderate, or low; the overall risk rating based upon the risk scale; and the recommended controls to mitigate the risk
- A summary that includes the number of high, moderate, and low findings and provides a list of prioritized action items based upon the findings.

The assessment shall be documented in a report that follows the NRC Template for Risk Assessment Report found in Appendix K. The report shall be delivered in draft form and then in final form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

The Contractor will track any residual risk in the Plan Of Action and Milestones (POA&M). The Contractor shall document the results of the process. This shall include documenting the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk. The goal is for NRC and Contractor personnel to remediate all high and moderate security findings, and track the remaining security findings in the POA&M.

Task 1.14 Develop System Security Plan

The Contractor shall develop a System Security Plan (SSP) for NSTS. The NSTS security plan shall be developed in accordance with NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*, NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, and the NRC IT Security Plan Template found in Appendix L The Contractor shall identify within the SSP the necessary security controls required to protect the NSTS, citing the security controls that are in place, those that are planned, and those that are not applicable. Where the NSTS relies upon a control that is provided by another system (e.g., the NRC LAN/WAN), the specific control being relied upon shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures, or NSTS-specific policy or procedures.

The SSP shall be documented in a report that follows the NRC Template for System Security Plan. The report shall be delivered in draft form and then in pre-System Security Test and Evaluation (ST&E) form after NRC comments are incorporated. The ST&E must be conducted by an independent party. NRC will have the ST&E conducted by a separate IV&V Contractor who will provide the ST&E report. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system security plan as final after completion of the ST&E test report to reflect validated in-place and planned controls. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

Task 1.15 Develop IT Contingency Plan and Perform Testing

The Contractor shall develop a contingency plan for the NSTS. The NSTS contingency plan shall be developed in accordance with NIST SP 800-34 *Contingency Planning Guide for Information Technology Systems*, NIST SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*, and the NRC Contingency Plan (CP) Template found in Appendix M. The Contractor shall provide detailed procedures for the notification and activation phase, recovery operations, and return to normal operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system contingency plan shall also contain sufficient personnel contact information to enable contact at all times, vendor contact information to enable contact at all times, equipment (hardware and software) and specification information to enable reconstitution of the system from scratch, all service level agreements and memoranda of understanding, the IT standard operating procedures for the system, identification of any systems that this system is dependent upon along with references for the applicable contingency plans, references to the emergency management plan and occupant evacuation plan, and references to the appropriate continuity of operations plan.

The system contingency plan shall be documented in a report that follows the NRC Template for System Contingency Plan. The report shall be delivered in draft form and then in pre-Test form after NRC comments are incorporated. The NRC IT Security staff review of the draft is required to ensure compliance. The Contractor shall update the system contingency plan after completion of the contingency plan test report to reflect validated information. The NRC Senior IT Security Officer must approve the final to enable system accreditation.

Prior to NSTS deployment, the Contractor shall perform system contingency testing in compliance with the NRC-approved test plan.

Task 1.16 Develop System Test Plan and Testing Scripts

The Contractor shall develop a System Test Plan (STP) for NSTS Task 1 functionality in accordance with section 7.4.3 of this PBSOW. Within the STP, the Contractor shall clearly detail the approach for ensuring independence of testing from the development team, in particular mitigating the risk of members of the development team introducing biases into the QC process. System test documentation shall consist of the Rational TestManager test plan and test cases along with a supplemental document following the template attached in Appendix N.

Task 1.17 Conduct System Test

Prior to delivery for NRC acceptance, the Contractor shall successfully complete system testing of NSTS Task 1 functionality and deliver to the NRC a Test Evaluation Summary, following the PMM template attached in Appendix O. As with other Contractor activities, the NRC reserves the right to have NRC personnel and the NRC IV&V team observe system testing. The Contractor shall provide any hardware tokens needed to perform contractor and NRC testing prior to production deployment.

Task 1.18 Develop Workshop Materials

Prior to implementation of the initial NSTS (Task 1 functionality), the NRC will offer a total of six four-hour licensee workshops and Agreement State-focused presentations in various parts of the country to discuss the NSTS regulations and demonstrate use of the system. The Contractor shall prepare all software and other needed materials and deliver system demonstrations and presentations about the system during these workshops.

Task 1.19 Develop User Guide and Training Materials

The Contractor shall develop materials suitable for providing 2-day training on source tracking for approximately 50 staff; four-hour training on import/export notification functions for 15 staff; and four-hour overview training for 100 staff. Those trained will include NRC staff and other individuals who will be the primary users of the system. These materials shall include an NSTS User Guide. In addition, the Contractor shall create, maintain, and update CBT modules for use by new NRC staff and external users needing to learn about their NSTS role after the initial training sessions have ended.

In the role-based CBT modules, the Contractor shall address the functions of the Licensee and Licensing Agency user communities as outlined in the use cases (Appendix B). While not included in the CBT portfolio, the contractor shall provide detailed user manuals to cover training needs of the System Administrator user functions. The Contractor shall ensure that both a CBT module and training materials for user training workshops explicitly cover the user registration process including obtaining credentials and use of the hardware token.

The Contractor shall submit all training plans and materials to the government for review and approval. The Contractor shall address all NRC comments to the satisfaction of the NRC project manager in producing the final version of the training plans, materials, and CBT modules.

While most external users of the system (e.g., other federal agencies, licensees, and A/S agencies who access the system via the Web interface) will not receive formal training, the Contractor shall ensure that the NSTS Web interface includes user-friendly navigation tools, online system help, and online reference to relevant NSTS regulatory material.

Task 1.20 Install Acceptance Test System at ASP

After System Test in the development environment, the Contractor shall install the system at the ASP for use in acceptance testing and training. The Contractor shall also work with the NRC staff to ensure that any needed NRC network system installation activities are accomplished in order for NRC staff to access the system at the ASP. If NRC network or desktop software is required, the Contractor shall provide system installation instructions and other information to government staff, as only NRC Office of Information Services (OIS) representatives are permitted to install such software. In addition, Contractor staff may be required to work with NRC staff during non-standard work hours to ensure that software installation activities do not disrupt business area activities.

Task 1.21 Support Acceptance Testing

The NRC will perform acceptance testing of Task 1 functionality, using NRC personnel and members of the IV&V team. The acceptance test plan and test cases will test Contractor-provided software, using the full initial NSTS production database created under Task 1.12. The Contractor shall be prepared to host acceptance testing at the Contractor facility and to provide all technical support required to set up and run acceptance tests using the Rational test tool suite. In particular, the Contractor shall also support definition of all user accounts to support role-based NRC tests. The Contractor shall also be prepared to provide system demonstrations and/or informal training of personnel who are to be involved in the acceptance testing.

Task 1.22 Conduct Engineering Review

The Contractor shall prepare and deliver a comprehensive engineering review for senior NRC management and SafeSource stakeholders that fully describes the system development and integration activities which the Contractor has completed.

Task 1.23 Conduct Workshops
The Contractor shall deliver system demonstrations and/or presentations about NSTS during six four-hour licensee workshops and Agreement State-focused presentations in various parts of the country. The Contractor shall provide at least two Web-enabled computers at each workshop and ensure that participants are able to access appropriate NSTS functions using these computers. The Contractor should assume two people traveling to each of the six workshop locations. The NRC must approve all Contractor-proposed workshop locations. The Contractor proposal shall include all costs of hosting the workshops (e.g., conference facility and equipment rental).

Task 1.24 Support Development of System Accreditation Documentation
The Contractor shall support the NRC staff and other Contractors tasked to develop a System Certification and Accreditation Report for the NSTS in accordance with the Computer Security Act of 1987, Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*; and NRC Management Directive 12.5. The IV&V Contractor having performed the System Test & Evaluation (ST&E) and the Contingency Plan Test will coordinate development of the System Accreditation documentation package. The Contractor shall provide the support required to ensure that all documentation is adequate to ensure that the NRC receives full certification and accreditation. The Contractor will be required to deliver briefings (as needed) to the IV&V Contractor.

System certification is the declaration by the system owner and information owner that the system has a current risk assessment, system security plan, system security test and evaluation plan, system security test and evaluation report, system contingency plan, system contingency plan test report, and a plan to resolve issues raised during system certification; and that the security controls listed in the system security plan have been assessed using the assessment methods and procedures described in the system security test and evaluation report and the contingency plan report to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The plan to resolve issues raised during system certification describes the corrective measures that have been implemented or are planned to address any deficiencies in the security controls for the information system and to reduce or eliminate known vulnerabilities.

The security certification package documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system. All required documentation must be provided to the IT security office in both hard copy and electronically in MS Word or WordPerfect. The IT security office will place the documents into ADAMS. The security certification package contains the following documents:

(1) current risk assessment;
(2) current security plan;
(3) current security test and evaluation (ST&E) plan and full test report;
(4) current contingency plan;
(5) current test results from full exercise of the contingency plan (NOT a tabletop test);(6) the plan to resolve issues resulting from the risk assessment, security plan, ST&E test results, and contingency plan test results

Task 1.25 Support Roll-out Planning

The Contractor shall support NRC staff and Contractors tasked with planning roll-out to NRC and to other system users who are licensees. This will include support for development of roll-out plans, training logistics, desk procedures, and correspondence with licensees.

Task 1.26 Conduct Readiness Review Demonstration
After NRC acceptance testing has been completed and required changes have been addressed and re-tested, the Contractor shall conduct a readiness review session with NRC and present the results of all activities, findings, and products developed during the engineering phase. The Readiness Review Demonstration shall group topics as logically as possible to facilitate comprehensive yet succinct issue coverage.

Task 1.27 Roll-out System to NRC (Includes Production Install & Training)
The Contractor shall perform all activities required to roll-out the initial NSTS to the NRC user community. The Contractor shall install and test NSTS in its production environment at the ASP, and work with NRC staff to facilitate smooth and efficient installation or configuration of any components needed on the NRC network or user workstations.

The Contractor shall provide two-day training on source tracking for approximately 50 staff; four-hour training on import/export notification functions for 15 staff; and four-hour overview training for 100 staff. The Contractor shall fulfill these training requirements through at least 12 separate training events.

Those trained will include NRC and other individuals who will be the primary users of the system. Training shall be conducted at times and dates acceptable to the NRC project manager.

The Contractor shall conduct all training to ensure that users and stakeholders are trained "just in time" to ensure there is no loss of time between completion of the training and availability of the system.

Task 1.28 Support Licensee Start-up
The NRC will correspond with parties who will be required to report to the NSTS, ensuring they receive digital certificate credentials and are prepared to access the system, verify and update their initial source inventory (entered into the system as a result of Task 1.12 Conduct Data Conversion), and begin recording source tracking transactions. The Contractor shall provide all technical support required to facilitate smooth and efficient use of the system by this licensee group. This includes developing and distributing a guide for formatting and submission of electronic data files, defining user accounts, and performing trouble-shooting. The Contractor shall also develop an Operational Guide.

The purpose of the Operational Guide is to document system usage and procedures for operations under routine and exceptional conditions. Within the Operational Guide, the Contractor shall address procedures for:

- System installation and configuration;
- Rules of conduct, including common operations such as opening and closing user accounts;
- System monitoring and reporting; and
- System archiving and relocation

Task 1.30 Develop System Refinement Recommendations
The Contractor shall provide a report containing its recommendations for changes to be made to the NSTS infrastructure, focusing in particular on the production system.

Task 1.31 Support Lessons Learned Study
In compliance with the Clinger-Cohen Act, the NRC will conduct an independent lessons learned study of this project. As the SafeSource Phase II project will potentially involve two production system deployments (Task 1 and Task 2 functions), the initial lessons learned study will be later amended as appropriate.

The Contractor shall participate in interviews and provide documentation as requested by the lessons learned study authors. The Contractor will be asked to offer recommendations and comments on a broad range of project aspects, including, but not limited to the feedback from the users and stakeholders; roll-out experiences; security enhancements suggested by independent evaluation.

Task 1.32 Support Security Architecture Analysis
The Contractor shall support NRC efforts to ensure optimal NSTS system security. In response to emergent security risks and development of new security technologies, the Contractor shall conduct market research and perform analyses to identify products that may strengthen the NSTS security architecture. Upon receipt of NRC direction, the Contractor shall revise all NSTS artifacts wherein the pertinent security architecture elements are reflected.

Deliverables

Exhibit 5-3 provides a list of Contractor deliverables for Task 1, along with expected delivery dates. *Deliverables listed in italics are delivery of support rather than work products.*

Exhibit 5-3: Task 1 Deliverables

WBS	Task No.	Deliverables	Proposed Due Date
1.2.6.1	1.3	Quality Assurance Plan - Draft V1.0	Task 1 Start (T1) + 63
1.2.6.4	1.7	Configuration Management Plan - Draft V1.0	T1 + 76
1.2.6.3	1.3	Quality Assurance Plan - Final V1.0	T1 + 77
1.2.6.7	1.2	Project Risk Management Plan - Draft V1.0	T1 + 84
1.2.6.10	1.2	Software Development Plan - Draft V1.0 (Initial)	T1 + 84
1.2.1.2	1.5	Requirements Validation Summary of Findings - Draft & Final V1.0	T1 + 85
1.2.1.3	1.5	Proposed Revisions to Requirements - Draft V1.0	T1 + 85
1.2.6.6	1.7	Configuration Management Plan - Final V1.0	T1 + 90
1.2.6.9	1.2	Project Risk Management Plan - Final V1.0	T1 + 98
1.2.1.5	1.5	Proposed Revisions to Requirements - Final V1.0	T1 + 99
1.2.6.12	1.2	Software Development Plan - Final V1.0 (Initial)	T1 + 102
1.2.6.13	1.2	Software Development Plan - Draft V2.0 (After requirement validation)	T1 + 116
1.2.6.15	1.2	Software Development Plan - Final V2.0	T1 + 132
1.2.4.2	1.13	System Security Risk Assessment (incl. strategies to address risks) - Draft V1.0	T1 + 145
1.2.3.1	1.16	System Test Plan - Draft V1.0 (Test Strategy)	T1 + 147
1.2.3.3	1.16	System Test Plan - Final V1.0 (Test Strategy)	T1 + 173
1.2.2.2	1.8	Detailed Design Model - Database - Draft V1.0	T1 + 188
1.2.4.4	1.13	System Security Risk Assessment - Final V1.0	T1 + 188
1.2.2.5	1.8	Detailed Design Model - User Interface - Draft V1.0	T1 + 195
1.2.2.8	1.8	Detailed Design Model - UML (All components) -Draft V1.0	T1 + 197
1.2.2.9	1.8	Detailed Design Model - Supplemental - Draft V1.0	T1 + 197
1.2.2.10	1.9	System Architecture Document - Draft V1.1	T1 + 203
1.2.2.4	1.8	Detailed Design Model - Database - Final V1.0	T1 + 208
1.2.4.5	1.14	System Security Plan - Draft V1.0	T1 + 210
1.2.2.7	1.8	Detailed Design Model - User Interface - Final V1.0	T1 + 215
1.2.2.12	1.8	Detailed Design Model - UML (All components) -Final V1.0	T1 + 223
1.2.2.12	1.8	Detailed Design Model - Supplemental - Final V1.0	T1 + 223
1.2.2.12	1.9	System Architecture Document - Final V1.1	T1 + 223
1.3.1.1	1.12	Data Conversion Design Documentation - Draft V1.0	T1 + 228
1.2.6.21	1.6	Deployment Plan - Draft V1.0 (Elaboration phase)	T1 + 232
1.3.1.3	1.12	Data Conversion Design Documentation - Final V 1.0	T1 + 237
1.2.6.16	1.2	Software Development Plan - Draft V3.0 (Design revision)	T1 + 237
1.3.3.1	1.8	Detailed Design Model - Database - Draft V2.0 (Design revision)	T1 + 251
1.3.3.2	1.8	Detailed Design Model - User Interface - Draft V 2.0 (Design revision)	T1 + 251
1.3.3.3	1.8	Detailed Design Model - UML (All components) -Draft V2.0	T1 + 251
1.2.6.23	1.6	Deployment Plan - Final V1.0 (Elaboration phase)	T1 + 251
1.3.3.4	1.8	Detailed Design Model - Supplemental Design- Draft V2.0 (Design revision)	T1 + 253
1.2.4.7	1.14	System Security Plan Final V1.0	T1 + 253
1.2.6.18	1.2	Software Development Plan - Final V3.0 (After design revision)	T1 + 256
1.3.10.2	1.18	Workshop Materials - Draft V1.0	T1 + 271

WBS	Task No.	Deliverables	Proposed Due Date
1.3.11.1	1.13	System Security Risk Assessment Report - Draft V2.0	T1 + 271
1.3.1.4	1.12	Data Conversion Scripts - V1.0	T1 + 278
1.3.3.6	1.8	Detailed Design Model - Database - Final V2.0 (Design revision)	T1 + 281
1.3.3.6	1.8	Detailed Design Model - User Interface - Final V 2.0 (Design revision)	T1 + 281
1.3.3.6	1.8	Detailed Design Model - UML (All components) -Final V2.0	T1 + 281
1.3.3.6	1.8	Detailed Design Model - Supplemental Design- Final V2.0	T1 + 281
1.3.10.4	1.28	Operational Guide, Draft V1.0	T1 + 284
1.3.1.5	1.12	Data Conversion Result Report and Related Documentation (incl. Test Plan, Scripts, etc.) - Draft V1.0	T1 + 285
1.3.12.2	1.2	Software Development Plan - Draft V4.0 (Construction Phase)	T1 + 286
1.2.4.11	1.15	IT Contingency Plan and Test - Draft V1.0	T1 + 286
1.3.1.7	1.12	Data Conversion Result Report and Related Documentation (incl. Test Plan, Scripts, etc.) - Final V1.0	T1 + 294
1.3.11.4	1.14	System Security Plan - Draft V2.0	T1 + 298
1.3.3.8	1.9	System Architecture Document - Draft V2.0 (w/ System Design)	T1 + 299
1.3.2.1	1.12	Data Conversion Design Documentation - Draft V 2.0 (Updated Design based on Results)	T1 + 301
1.3.8.1	1.16	System Test Plan - Draft V2.0	T1 + 301
1.3.12.4	1.2	Software Development Plan - Final V4.0 (Construction Phase)	T1 + 302
1.3.10.1	1.19	User Guide - Draft V1.0	T1 + 302
1.3.2.3	1.12	Data Conversion Design Documentation - Final V 2.0 (Updated Design based on Results)	T1 + 312
1.3.3.10	1.9	System Architecture Document - Final V2.0 (w/ System Design)	T1 + 313
1.3.11.3	1.13	System Security Risk Assessment Report - Final V2.0	T1 + 314
1.3.10.3	1.19	Training Material Draft V1.0	T1 + 315
1.3.2.4	1.12	Data Conversion Scripts - V2.0	T1 + 319
1.3.2.5	1.12	Data Conversion Result Report and Related Documentation (incl. Test Plan, Scripts, etc.) - Draft V2.0	T1 + 321
1.3.8.3	1.16	System Test Plan - Final V2.0	T1 + 327
1.2.4.13	1.15	IT Contingency Plan and Test - Final V1.0	T1 + 328
1.3.5.2	1.11	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection, Construction Feature Set #1	T1 + 328
1.3.2.7	1.12	Data Conversion Result Report and Related Documentation (incl. Test Plan, Scripts, etc.) - Final V2.0	T1 + 330
1.3.11.6	1.14	System Security Plan - Final V2.0	T1 + 340
1.3.6.2	1.11	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection, Construction Feature Set #2	T1 + 340
1.3.10.6	1.19	User Guide - Final V1.0	T1 + 342
1.3.10.6	1.18	Workshop Materials - Final V1.0	T1 + 342
1.3.10.6	1.19	Training Material - Final V1.0	T1 + 342
1.3.10.6	1.28	Operational Guide - Final V1.0	T1 + 342
1.4.3.1	1.19	User Guide Draft V2.0	T1 + 355
1.4.3.3	1.28	Operational Guide Draft V2.0	T1 + 356
1.4.3.4	1.28	Guide for Formatting and Submission of Electronic Data Files - Draft V1.0	T1 + 356
1.3.11.10	1.15	IT Contingency Plan - Draft V2.0 (for Security Testing)	T1 + 356
1.3.8.4	1.16	System Test Script - Final (Feature Set #1)	T1 + 356

WBS	Task No.	Deliverables	Proposed Due Date
1.3.8.5	1.16	System Test Script - Final (Feature Set #2)	T1 + 364
1.4.3.2	1.19	Training Material Draft V2.0	T1 + 368
1.4.3.6	1.19	User Guide Final V2.0	T1 + 382
1.4.3.6	1.28	Operational Guide Final V2.0	T1 + 382
1.4.3.6	1.19	Training Material Final V2.0	T1 + 382
1.4.3.6	1.28	Guide for Formatting and Submission of Electronic Data Files - Final V1.0	T1 + 382
1.3.7.2	1.11	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection, Construction Feature Set #3	T1 + 386
1.3.11.12	1.15	IT Contingency Plan - Final V2.0 (for Security Testing)	T1 + 398
1.3.12.5	1.6	Deployment Plan - Draft V2.0 (Construction phase)	T1 + 407
1.3.8.7	1.11	Deployed System (Unit and integration tested), Build for System Testing	T1 + 407
1.3.8.6	1.16	System Test Script - Final (Feature Set #3)	T1 + 414
1.3.12.7	1.6	Deployment Plan - Final V2.0 (Construction phase)	T1 + 425
1.3.8.9	1.17	System Test Evaluation Summary	T1 + 447
1.4.5.4	1.15	IT Contingency Test Report - Draft V1.0 (for Certification)	T1 + 454
1.3.9.2	1.11	Deployed System (Unit and integration tested), Build for IV&V Inspection, Addresses System Testing Issues	T1 + 456
1.4.5.5	1.14	System Security Plan - Draft V3.0 (for System Certification)	T1 + 461
1.4.5.7	1.14	System Security Plan - Final V3.0 (for System Certification)	T1 + 467
1.4.5.7	1.15	IT Contingency Test Report - Final V1.0 (for Certification)	T1 + 467
1.4.2.2	1.11	Deployed System (Unit and integration tested), Build for IV&V Inspection, Addresses User Acceptance Testing Issues	T1 + 531
1.4.7.3	1.12	Data Conversion and Conversion Documentation - Final V3.0 (Production Environment conversion results)	T1 + 547
1.4.7.4	1.11	Deployed System (Unit and integration tested) - Final V1.0	T1 + 547
1.4.9.1	1.30	System Refinement Recommendations	T1 + 589

5.4 Optional Task 2: Develop Enhanced NSTS

Scope of Work

The enhanced system will add the following functionality:

- the ability for NRC to record and track import consents and import/export notifications made by NRC import/export licensees;
- the ability to link notifications to import and export transfer and receipt transactions, and report import and export related information;
- provide notifications required by DHS/Customs and Border Protection (CBP); and
- automated system interfaces, full reporting and alert capabilities, and reporting to additional federal agencies.

The enhanced NSTS will be deployed to all affected licensees simultaneously.

Schedule and Detailed Task Descriptions

The Task 2 schedule is presented in Appendix P and is reflected in the Exhibit 5-4 deliverable schedule. Detailed task descriptions are provided below.

Performance of the detailed tasks by the Contractor is non-negotiable. However, the Contractor may propose different task durations and to some extent revised task sequencing within the iterative PMM template context represented in Appendix P and Exhibit 5-4. In doing so, the Contractor shall maintain the key NRC milestones and meet all performance requirements described in Appendix A. In proposing a technical approach, the Contractor shall conform to the "Design and Implementation Controls" identified in Section 6. The Contractor is encouraged to propose a schedule that optimizes use of Contractor resources to provide for an earlier deployment date. In doing so, the Contractor shall not compress schedule intervals proposed for reviews and other activities to be conducted by personnel from the NRC, IV&V contractor or other agencies.

Task 2.1 Develop SDP, and Validate/Revise QAP, CMP, RMP, and SAD

The Contractor shall develop a Task 2 SDP or revise the original Task 1 SDP to include the Task 2 development. In revising the SDP, the Contractor shall specifically address the strategy for managing concurrent NSTS V2 development and NSTS V1 maintenance. This plan shall address plans for ensuring adequate staffing and ensuring software quality and stability. The Contractor shall review and assure that the contents of the Quality Assurance Plan (QAP), Configuration Management Plan (CMP), Risk Management Plan (RMP), and Software Architecture Document (SAD) developed in Task 1 are still valid given the approval for Task 2 work. The Contractor shall develop revised versions of these documents, where needed to provide for Task 2 work. In particular, the NRC expects that the SAD will require revision. The Contractor shall provide for a draft submission and a final edition of all newly developed or revised documents.

Task 2.2 Validate Requirements

The Contractor shall conduct an effort to validate the NSTS Task 2 requirements. In this effort, the Contractor shall hold workshops, conduct interviews, and otherwise obtain requirement specification concurrence from representatives of all stakeholder groups. The foundation for this effort is Appendix B, SafeSource Phase II Requirements Analysis. Following requirements validation, the Contractor shall submit to the NRC proposed revisions to requirements documentation, in particular the baseline use cases. The Contractor shall also deliver to the NRC a report summarizing the findings of the validation effort.

Task 2.3 Update Deployment Plan

The Contractor shall update and deliver to the NRC the Deployment Plan developed in Task 1, or a separate Deployment Plan, describing in detail the deployment of Task 2 functionally. In the Deployment Plan, the Contractor shall also identify the steps and procedures which the Contractor will employ to deploy the Task 2 functions to NRC users, including plans for training, and to support three groups of licensees as they start using the system in succession. In developing the deployment plan, the Contractor shall assume that the NRC rollout starts within 14 days after the Contractor conducts the Readiness Review Demonstration. The Deployment Plan shall address all issues regarding labor and other resources, timing, sequence and schedules.

Task 2.4 Update Detailed Design

The Contractor shall update the Task 1 detailed design models and Supplemental Design Document and deliver these to the NRC, describing the logical and physical design of Task 2 functionally. The Contractor shall follow NRC direction regarding NRC review of proposed

design model changes, allowing for NRC review prior to Contractor delivery of a final version addressing all NRC concerns.

Task 2.5 Conduct Design Review
The Contractor shall prepare and deliver a comprehensive design review for senior NRC management and SafeSource stakeholders that covers the enhanced NSTS capability (Task 2 functions) in the context of the entire system.

Task 2.6 Develop System
The Contractor shall construct system components that are needed to implement required Task 2 system functionality in accordance with the approved system design and validated requirements.

Should the Contractor propose a commercial off-the-shelf (COTS) product as part of the solution, the Contractor shall comply with the NMSS COTS Policy document in Appendix J. Furthermore, if both custom sub-systems and a COTS product are employed in the solution, the Contractor shall construct custom sub-systems in a way that does not interfere with the ability to deploy subsequent COTS version upgrades.

Task 2.7 Update System Security Risk Assessment
The Contractor shall conduct a risk assessment of the NSTS considering the addition of Release 2 functionality and shall update the System Security Risk Assessment Report, developed under Task 1. As part of this update, the Contractor shall update the strategy for addressing all identified NSTS security risks. The System Security Risk Assessment Report shall be completed following the guidance cited in Task 1.13 as it pertains to the new functions.

Task 2.8 Update System Security Plan
The Contractor shall update the System Security Plan (SSP) for NSTS developed in Task 1 to take into account the Task 2 functionality. The Contractor shall follow the process described for Task 1.14 as it pertains to the new functions.

Task 2.9 Update IT Contingency Plan and Test
The Contractor shall coordinate with the NRC Project Manager and the IV&V Contractor to determine if the changes to the NSTS resulting from the Task 2 effort have sufficiently impacted the Contingency Plan controls and procedures developed under Task 1.15. Significant impacts will require an update of the plan, re-training and re-testing of the plan. Such an update and re-testing must be fully documented with the resultant report containing a plan for resolving any new issues identified during the test. A significant update to the Contingency Plan will require the approval of the NRC Senior IT Security Officer.

Should the determination be made that the changes to the NSTS resulting from Task 2 do not have significant impacts on the CP controls or procedures, the resulting update can be accomplished and documented within the CP on a Record of Changes located at the front of the plan. An update to the plan that does not significantly impact the plan's controls and procedure will not require re-training or re-testing.

Task 2.10 Develop System Test Plan
The Contractor shall develop a System Test Plan (STP) for NSTS Task 2 functionality in accordance with section 7.4.3 of this PBSOW. Within the STP, the Contractor shall clearly detail the approach for ensuring independence of testing from the development team, in particular mitigating the risk of members of the development team introducing biases into the

QC process. System test documentation shall consist of the Rational TestManager test plan and test cases along with a supplemental document following the template attached in Appendix N.

Task 2.11 Conduct System Test
Prior to delivery for NRC acceptance, the Contractor shall successfully complete system testing of NSTS Task 2 functionality and deliver to the NRC a Test Evaluation Summary, following the PMM template attached in Appendix O. As with other Contractor activities, the NRC reserves the right to have NRC personnel and the NRC IV&V team observe system testing.

Task 2.12 Update User Guide and Training Materials
The Contractor shall develop materials suitable for providing a four-hour update on the new Task 2 functionality in the context of the entire system to be delivered to approximately 50 staff. Those trained will include NRC staff and other individuals who will be the primary users of the system. These materials shall include the NSTS User Guide updated to include the Task 2 functions. In addition, the Contractor shall update the CBT modules developed in Task 1, addressing Task 2 functionality for use by new staff needing to learn about their NSTS role after the initial training sessions have ended.

The Contractor shall submit all training plans and materials to the government for review and approval. The Contractor shall address all NRC comments to the satisfaction of the NRC project manager in producing the final version of the training plans, materials, and CBT modules.

While most external users of the system (e.g., other federal agencies, licensees, and A/S agencies who access the system via the Web interface) will not receive formal training, the Contractor shall ensure that the NSTS Web interface includes user-friendly navigation tools, online system help, and online reference to relevant NSTS regulatory material.

Task 2.13 Install Acceptance Test System at ASP
After System Test in the development environment, the Contractor shall install the updated system at the ASP for use in acceptance testing and training. If needed, he Contractor shall also work with the NRC's NMSS and OIS staff to ensure that any needed NRC network system installation activities are accomplished in order for NRC staff to access the system at the ASP. If NRC network or desktop software is required, the Contractor shall provide system installation instructions and other information to government staff, as only OIS representatives are permitted to install such software. In addition, Contractor staff may be required to work with NRC staff during non-standard work hours to ensure that software installation activities do not disrupt business area activities.

Task 2.14 Support Acceptance Testing
The NRC will perform acceptance testing of Task 2 functionality, using NRC personnel and members of the IV&V team. Acceptance test plans and test cases will test Contractor-provided software. The Contractor shall be prepared to host acceptance testing at the Contractor facility and to provide all technical support required to set up and run acceptance tests using the Rational test tool suite. In particular, the Contractor shall also support definition of all user accounts to support role-based NRC tests. The Contractor shall also be prepared to provide system demonstrations and/or informal training of personnel who are to be involved in the acceptance test.

Task 2.15 Conduct Engineering Review
The Contractor shall develop and deliver a comprehensive engineering review for senior NRC management and SafeSource stakeholders that fully describes the system development and integration activities which the Contractor has completed for Task 2.

Task 2.16 Support Update of System Accreditation Documentation
As required, the Contractor shall support the other NRC staff and Contractors tasked to develop any updates to the System Certification and Accreditation Report for the NSTS in accordance with the Computer Security Act of 1987, FIPS PUB 102, as well as various NRC Management Directives. The process is described in Task 1.24.

Task 2.17 Support Roll-out Planning
The Contractor shall support NRC staff and Contractors tasked with planning roll-out of Task 2 functions to NRC and to licensee users. This will include support to development of roll-out plans, training logistics, desk procedures, and correspondence with licensees.

Task 2.18 Conduct Readiness Review Demonstration
After NRC acceptance testing has been completed and required changes have been addressed and re-tested, the Contractor shall conduct a readiness review session with NRC and present the results of all activities, findings, and products developed. The Readiness Review Demonstration shall group topics as logically as possible to facilitate comprehensive yet succinct issue coverage.

Task 2.19 Roll-out System to NRC (Includes Production Install & Training)
The Contractor shall perform all activities required to roll-out the enhanced NSTS to the NRC user community. The Contractor shall install and test NSTS in its production environment at the ASP, and work with NRC staff to facilitate smooth and efficient installation or configuration of any components needed on the NRC network or user workstations.

The Contractor shall provide four-hour update training on new system features for approximately 50 staff. Those trained will include NRC and other individuals who will be the primary users of the system. The Contractor shall fulfill these training requirements through at least five separate training events. Training shall be conducted at times and dates agreeable to the NRC project manager.

The Contractor shall schedule and conduct all training to ensure that users and stakeholders are trained "just in time" to ensure there is no loss of time between completion of the training and availability of the system.

Task 2.20 Support Roll-out to External User Groups
The Contractor shall provide all technical support required to facilitate smooth and efficient adoption of new features by licensees, and users from other organizations such as Agreement States and other government agencies.

Task 2.21 Support Roll-out to Other Agency Users
The Contractor shall provide all technical support required to facilitate smooth and efficient adoption of new features by this group.

Task 2.22 Support Lessons Learned Study
In compliance with the Clinger-Cohen Act, the NRC will update the independent lessons learned study developed in Task 1. The Contractor shall participate in interviews and provide

documentation as requested by the lessons learned study authors. The Contractor will be asked to offer recommendations and comments on a broad range of project aspects, including, but not limited to the feedback from the users and stakeholders; roll-out experiences; security enhancements suggested by independent evaluation.

Deliverables

Exhibit 5-4 provides a list of Contractor deliverables for Task 2, along with expected delivery dates. *Deliverables listed in italics are delivery of support rather than work products.*

Exhibit 5-4: Task 2 Deliverables

WBS	Task No.	Deliverables	Proposed Due Date
1.2.5.1	2.1	Quality Assurance Plan - Draft V2.0	Task 2 Start Date (T2) + 3
1.2.5.3	2.1	Quality Assurance Plan - Final V2.0	T2 + 3
1.2.5.4	2.1	Configuration Management Plan - Draft V2.0	T2 + 3
1.2.5.7	2.1	Project Risk Management Plan - Draft V2.0	T2 + 8
1.2.5.6	2.1	Configuration Management Plan - Final V2.0	T2 + 10
1.2.5.9	2.1	Project Risk Management Plan - Final V2.0	T2 + 14
1.2.5.10	2.1	Software Development Plan - Final V5.0	T2 + 37
1.2.1.2	2.2	Summary Findings of Requirements Validation - Draft & Final V1.0	T2 + 40
1.2.1.3	2.2	Proposed Requirement Changes - Draft V1.0	T2 + 42
1.2.3.2	2.7	System Security Risk Assessment - Draft V3.0	T2 + 45
1.2.1.5	2.2	Proposed Requirement Changes - Final V1.0	T2 + 49
1.2.5.12	2.1	Software Development Plan - Final V5.0	T2 + 49
1.2.5.13	2.1	Software Development Plan - Draft V6.0	T2 + 55
1.2.5.15	2.1	Software Development Plan - Final V6.0	T2 + 59
1.2.3.4	2.7	System Security Risk Assessment - Final V3.0	T2 + 77
1.2.2.2	2.4	Database Design - Draft V3.0	T2 + 94
1.2.2.4	2.4	Database Design - Final V3.0	T2 + 104
1.2.2.9	2.4	Supplemental Design Document - Draft V3.0	T2 + 112
1.2.2.8	2.4	Design Models - Draft V3.0	T2 + 113
1.2.2.5	2.4	User Interface Design - Draft V3.0	T2 + 115
1.2.2.10	2.4	System Architecture Document (SAD) - Draft V3.0	T2 + 119
1.2.2.12	2.4	Design Models, Supplemental Design Document and SAD - Final V3.0	T2 + 133
1.2.2.7	2.4	User Interface Design - Final V3.0	T2 + 133
1.2.3.5	2.8	System Security Plan - Draft V4.0	T2 + 133
1.2.5.21	2.3	Deployment Plan - Draft V1.0	T2 + 134
1.2.5.23	2.3	Deployment Plan - Final V1.0	T2 + 134
1.4.3.3	2.12	Operational Support Materials - Draft V3.0	T2 + 135
1.2.5.16	2.1	Software Development Plan - Draft V7.0	T2 + 136
1.2.5.18	2.1	Software Development Plan - Final V7.0	T2 + 142

WBS	Task No.	Deliverables	Proposed Due Date
1.4.3.1	2.12	System Support Materials - Draft V3.0	T2 + 143
1.4.3.2	2.12	Training Materials - Draft V3.0	T2 + 147
1.3.7.2	2.1	Software Development Plan - Draft V8.0	T2 + 154
1.2.3.7	2.8	System Security Plan - Final V4.0	T2 + 162
1.3.7.4	2.1	Software Development Plan - Final V8.0	T2 + 162
1.3.4.1	2.1	System Test Plan - Draft V1.0	T2 + 163
1.4.3.5	2.12	System Support Materials, Training Materials, and Operational Support Materials - Final V3.0	T2 + 168
1.3.6.1	2.9	Contingency Plan - Draft V3.0	T2 + 177
1.3.2.2	2.6	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection, Construction Feature Set #1	T2 + 185
1.3.4.3	2.1	System Test Plan - Final V1.0	T2 + 189
1.3.6.3	2.9	Contingency Plan - Final V3.0	T2 + 189
1.3.4.4	2.1	System Test Scripts (Feature Set #1)	T2 + 217
1.3.3.2	2.6	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection, Construction Feature Set #2	T2 + 273
1.3.7.5	2.3	Deployment Plan - Draft V2.0	T2 + 288
1.3.4.6	2.6	Deployed System (Unit and integration tested), Interim Build for System Testing and ST&E Evaluation	T2 + 296
1.3.7.7	2.3	Deployment Plan - Final V2.0	T2 + 300
1.3.4.5	2.1	System Test Scripts (Feature Set #2)	T2 + 302
1.4.5.4	2.9	Contingency Test Report - Draft V2.0	T2 + 324
1.4.5.5	2.9	Contingency Test Report - Final V2.0	T2 + 328
1.3.4.8	2.11	System Test Evaluation Summary	T2 + 335
1.3.5.2	2.6	Deployed System (Unit and integration tested), Interim Build for IV&V Inspection	T2 + 345
1.4.2.2	2.6	Deployed System (Unit and integration tested), for IV&V Inspection	T2 + 392
1.4.6.4	2.6	Deployed System Final Production Build	T2 + 392

5.5 Task 3: Operational Support

5.5.1 Task 3.1 Operational Support for the NSTS and WBL – Base Period

General Information

The Contractor shall propose a schedule for beginning operational support. In this schedule, the Contractor shall ensure availability of the production NSTS platform and infrastructure for NRC acceptance testing of NSTS V1. The Contractor shall also minimize costs to the NRC due to premature commencing of operational support. In compliance with the NRC accepted schedule, the Contractor shall begin work under this task, activating all hosting facilities and providing comprehensive NSTS operational support services.

While the NRC expects that the NSTS and WBL can be hosted together without revising the WBL infrastructure, the Contractor shall propose any changes needed to ensure reliable performance of both systems. In adopting the WBL infrastructure specifications, the Contractor shall be responsive to different telecommunication and security requirements of each system. The Contractor shall support the NRC goal of maximizing efficiencies in sharing of software

licenses and hardware, where appropriate. Detailed specifications of the NSTS and WBL operating environments are found in Section 6.

Within the scope of this task, the contractor shall provide comprehensive disaster recovery support, including routine system and data backups, off-site storage of backup media, disaster recovery rollover accommodations at a geographically disparate hosting facility. The contractor disaster recovery strategy shall ensure that disaster recovery sites are located a sufficient distance from the primary hosting site so as to mitigate the effect of regional events (e.g., a partial power grid failure, or natural disaster). The contractor shall propose a schedule for periodic testing of the disaster recovery plan, applying representative scenarios of different levels of service disruption.

All hosting and disaster recovery sites shall be located within the continental United States. The contractor shall ensure that all hosting and disaster recovery sites comply with NRC security requirements as governed by the relative data sensitivity and system availability needs. The contractor shall ensure that all staff with access to the NSTS hosting and disaster recovery environments shall be eligible for NRC security clearance.

The contractor shall provide NRC personnel and their contractors access to all contractor facilities, systems, and hardware to permit security accreditation testing, evaluation, and general review of compliance with contract requirements. The primary purpose of these visits will be to support system security certification in accordance with related National Institute of Standards and Technology (NIST) guidance and other applicable security guidance. The contractor shall also provide all support needed for NRC inspection, documentation, and testing of facilities and systems related with security certification.

The Contractor shall express their understanding of the NRC hosting and operational support requirements in the form of a service level agreement (SLA) between the Contractor and the NRC. Should the Contractor obtain these services through a partnering arrangement, the Contractor shall present to the NRC evidence of supporting SLAs between the Contractor and their related partner(s).

5.5.2 WBL Support

When the NRC elects to transfer WBL hosting and operational support from the current provider, the Contractor shall provide support to ensure transition of operations without disrupting WBL use. This support shall include Contractor coordination with the current ASP, telecommunication service providers, the NRC, and other affected WBL stakeholders.

General WBL users will access the system through a web interface using common web browser technologies. NRC users will access advanced WBL functions using VPN technology to connect NRC facilities to the WBL hosting site. VPNs specified by the Contractor shall support both extended network or user-based sessions, as required by the NRC.

5.5.2.1 WBL Hardware

Web Server Cluster - The Web Server cluster will provide Web services for all licensees' users and State Agencies users. The Web server will use the Apache application server software running on a Linux Operating System platform.
Application Server Cluster – The Application Server cluster will use Oracle's 9iAS Application Server and Orion Application Server. These services run on a Linux Operating system platform.

Database Server Cluster - The Database Server Cluster will host the Oracle 10g Database Management System (DBMS). The WBL will be implemented using Oracle Real Application Clusters (RAC).

5.5.2.2 WBL Software

Apache Web Server
LicenseEase COTS Product
Oracle DBMS
Orion Application Server – The Orion application server supports eGateway public access functions with its required JDK level 1.4.
Oracle Application Server - The Oracle Application Server is used to implement the business layers of LicenseEase.

5.5.2.3 WBL Telecommunications

While the Contractor shall provide support in acquiring and setting-up all telecommunication infrastructure, for non-NRC sites, the Contractor shall include in their proposal only the cost of any infrastructure needed to connect sites to operational support services (e.g., toll free lines, VPN support). NSTS telecommunication requirements are more extensive than those for the WBL and are detailed in Section 6.3.3. The Contractor shall propose all hardware, software, services and recurring costs required to provide and install the VPN appliance(s) and support a point-to-point VPN between the NRC headquarters and hosting site, DOE headquarters and the hosting site, and any similar support required for maintenance Contractor and user support Contractor sites. The Contractor shall also propose necessary infrastructure to host a Lightweight Directory Access Protocol (LDAP) repository to support a single sign-on for externally hosted NRC systems.

5.5.2.4 Detailed Operational Support Requirements

In providing operational support under this task, the Contractor shall:

- obtain, provide, and manage the ASP and all other telecommunication infrastructure and services needed to support access to the NSTS and WBL;
- provide all needed support for connectivity to NRC facilities and DOE headquarters;
- provide system availability support and trouble shooting support between the hours of 7:30 am and 5:30 pm Eastern Time, except weekends and US federal holidays;
- obtain all telecommunication services to allow users to obtain user support over the internet and by US toll-free telephone number(s);
- ensure support of all performance and operational requirements of both the NSTS and WBL, as detailed in Sections 3.3, 3,4 and Appendix A;
- provide comprehensive support for the Oracle databases and Application Server software, including backup/recovery services, performance monitoring, and version upgrades;
- support access by and be responsive to software maintenance Contractors and user support Contractors;
- include in the cost proposal all costs, initial and recurring, related to operational support;
- log in the NRC ClearQuest change management system all reports of potential problems with NSTS or WBL software as well as any user requested changes/enhancements reported to the operational support staff;
- investigate all user reports of apparent inaccessibility of the systems; and

- report to the NRC Project Manager any user-reported issue that cannot be resolved within four business hours and is diminishing or preventing access to and use of all system functions;

The Contractor shall ensure that the NSTS infrastructure and applications are reliable and available to users on a continuous basis. The Contractor shall monitor availability of all parts of the production system and report up time statistics to the NRC Project Manager on a monthly basis. Should any part of the production system experience unacceptable down time as defined in Section 3.3.5 of this PBSOW, the Contractor shall report this to the NRC Project Manager within one business day, including a proposed plan to prevent recurrence of the problem. Upon NRC acceptance, the Contractor shall implement necessary actions to address the cause of the down time. The Contractor shall incur all costs related to addressing issues of unacceptable down time.

In addition to general system availability, the Contractor shall ensure that all security aspects of the system are monitored. The Contractor shall complete the Security Self-Assessment (Appendix A of NIST Special Publication 800-26, "Self-Assessment Guide for Information Technology Systems") for SafeSource Phase I. The Contractor shall review the SafeSource Phase II Risk Assessment Reports and System Security Plans, other related documentation, and interview two to five NRC employees, as directed by the NRC Project Manager, to determine the status of each of the 17 control topic areas. The Contractor shall also determine the status of each control by quantifying the level of maturity of the control in one of the following categories:

Level 1 - Control objective documented in a security policy
Level 2 - Security controls documented as procedures
Level 3 - Procedures have been implemented
Level 4 - Procedures and security controls are tested and reviewed
Level 5 - Procedures and security controls are fully integrated into a comprehensive program

The Contractor shall use the General Accounting Office (GAO) Federal Information Systems Control Audit Methodology (FISCAM) as a guide when categorizing each of the controls into the appropriate maturity level. The Contractor shall analyze the results of the self assessment and document action plans that management can then use to remediate all controls that are categorized below level 5.

5.5.2.5 Earned Value Reporting

The Contractor shall track and report all operational support and hosting costs separately, by system (NSTS or WBL). In reporting these costs, the Contractor shall comply with all requirements described in Appendix S. Additionally, the contractor shall ensure that each WBS, as represented in Microsoft Project is decomposed to a sufficiently detailed level such that no task (work package) requires more than 80 or fewer than eight staff hours.

5.5.3 Optional task 3.2 Operational Support for the NSTS and WBL – Option Period 1

At the option of the NRC, the Contractor shall provide all support detailed under Task 3.1, for an additional year, following the Task 3.1 performance period.

5.5.4 Optional task 3.3 Operational Support for the NSTS and WBL – Option Period 2

At the option of the NRC, the Contractor shall provide all support detailed under Task 3.1, for an additional year, following the Task 3.2 performance period.

5.5.5 Optional task 3.4 Operational Support for the NSTS and WBL – Option Period 3

At the option of the NRC, the Contractor shall provide all support detailed under Task 3.1 for an additional year, following the Task 3.3 performance period.

5.6 Task 4: Maintenance

5.6.1 Task 4.1 NSTS Maintenance

Task 4.1.1 NSTS Maintenance – Base Period

Upon NRC acceptance of NSTS V1, the Contractor shall be prepared to provide the following maintenance support, as directed by the NRC, up to a resource level of 4,000 hours.

In providing maintenance, the Contractor shall comply with the prevailing NRC software change process. Documentation for the change process is included in the Appendix Q, OCIO Application Change Request System Guide. The Contractor shall not work on any change that is not logged and requested through the NRC ClearQuest tool. The Contractor shall not proceed with work on any change request unless directed by the NRC, as expressed in ClearQuest state transitions.

In performing maintenance, the Contractor shall comply with prevailing NRC CM requirements, in particular check-out/check-in procedures.

The NRC embraces release-based software maintenance. In support of this, the Contractor shall ensure that each maintenance system build has accompanying test plans, test evaluation summaries, and system documentation update activities as detailed under the NSTS development tasks.

The Contractor shall ensure that all maintenance staff have demonstrated skill, experience, and vendor certifications related to their role. The Contractor shall ensure that software engineers have at least two years experience in using the target development tools on systems of similar size and complexity. The Contractor shall ensure that software testers have formal training and no less than one year of experience in software testing. The Contractor shall also ensure that all maintenance staff are trained and experienced in all Rational tools applicable to their role in software maintenance.

During maintenance, the Contractor shall be responsive to the NRC IV&V team and shall support IV&V visits to the Contractor site and review of any Contractor products throughout the maintenance process. The Contractor shall support any testing that the NRC elects to perform in the Consolidated Testing Facility (CTF), within the NRC headquarters.

Optional task 4.1.2 NSTS Maintenance – Option Period 1

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.1.1, for an additional year, following the Task 4.1.1 performance period.

Optional task 4.1.3 NSTS Maintenance – Option Period 2

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.1.1, for an additional year, following the Task 4.1.2 performance period.

Optional task 4.1.4 NSTS Maintenance – Option Period 3

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.1.1, for an additional year, following the Task 4.1.3 performance period.

5.6.2 Task 4.2 WBL Maintenance

Optional task 4.2.1 WBL Maintenance – Base Period

Should the NRC elect to execute this task, the Contractor shall provide comprehensive software maintenance support for the WBL System, as directed by the NRC, up to a resource level of 2,500 hours.

At the direction of the NRC, the Contractor shall support transition of maintenance activities from the SafeSource Phase I development Contractor. This transition shall include a review of system artifacts and documentation.

In providing maintenance, the Contractor shall comply with the prevailing NRC software change process. Documentation for the change process is included in Appendix Q. The Contractor shall not work on any change that is not logged and requested through the NRC ClearQuest tool. The Contractor shall not proceed with work on any change request unless directed by the NRC, as expressed in ClearQuest state transitions.

In performing maintenance, the Contractor shall comply with prevailing NRC CM requirements, in particular check-out/check-in procedures.

The NRC embraces release-based software maintenance. In support of this, the Contractor shall ensure that each maintenance system build has accompanying test plans, test evaluation summaries, and system documentation update activities as detailed under the NSTS development tasks.

The Contractor shall ensure that all maintenance staff have demonstrated skill, experience, and vendor certifications, where available, related to their role. The Contractor shall ensure that software engineers and system administrators have demonstrated skill and experience in configuration of the Versa Systems LicenseEase and eLicense Gateway products. Should the proposed maintenance staff have less than one year of demonstrated experience in maintaining the Versa products, the Contractor shall provide a detailed approach through which the staff will be prepared to meet NRC needs under this task. In addition, the Contractor shall ensure that maintenance staff have at least two years experience supporting systems employing a three-tier architecture using Oracle Application Servers and the Oracle database engine. The Contractor shall ensure that software testers have formal training and no less than one year of experience in software testing. The Contractor shall also ensure that all maintenance staff are trained and experienced in all Rational tools applicable to their role in software maintenance.

During maintenance, the Contractor shall be responsive to the NRC IV&V team and shall support IV&V visits to the Contractor site and review of any Contractor products throughout the maintenance process. The Contractor shall support any testing that the NRC elects to perform in the Consolidated Testing Facility (CTF), within the NRC headquarters.

Deleted: April

Optional task 4.2.2 WBL Maintenance – Option Period 1

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.2.1, up to a resource level of 2,000 hours, for an additional year, following the Task 4.2.1 performance period.

Optional task 4.2.3 WBL Maintenance – Option Period 2

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.2.1, up to a resource level of 2,000 hours, for an additional year, following the Task 4.2.2 performance period.

Optional task 4.2.4 WBL Maintenance – Option Period 3

At the option of the NRC, the Contractor shall provide all support detailed under Task 4.2.1, up to a resource level of 2,000 hours, for an additional year, following the Task 4.2.3 performance period.

5.7 Task 5: NSTS User Support

Task 5.1 NSTS User Support – Base Period

Upon NRC acceptance of NSTS V1, the Contractor shall provide the full range of the support detailed under this task. When the NRC directs the Contractor to begin work under this task, the Contractor shall activate all facilities and telecommunication services needed to provide comprehensive support to the NSTS user community. The NSTS user community will include NRC headquarters, NRC regional offices, DOE headquarters, NRC Agreement States agencies, NRC and Agreement State licensees, and other concerned parties.

Deleted: While this task shall become active on or about December 20, 2006, the Contractor shall only provide support preparation work as approved by the NRC prior to NRC acceptance of NSTS V1.

Telecommunication infrastructure provided by the Contractor under this task shall include:

- at least two toll-free phone lines with roll-over to an answering system;
- broadband internet connectivity allowing the Contractor to access to the NRC ClearQuest software change request system; and
- any communication lines or infrastructure to allow the Contractor to access the NSTS to simulate user-provided scenarios and to provide support such as access control changes.

Deleted: (e.g., password resets)

The contractor shall specify, acquire, support installation of and pay recurring costs for any communication lines required for connection to an NRC facility.

Deleted: for

In providing user support under this task, the Contractor shall:

- assist all NSTS users in obtaining user accounts and maintaining those accounts;
- assist NSTS users in understanding and use of the system;
- directing users to appropriate NRC personnel for clarification or interpretation of NRC reporting regulations;
- provide data entry support for users who choose not to use the NSTS and who provide data by hard copy, fax or other means;
- provide a system for marking mail with the date received and for tracking data entry tasks to ensure timely completion;
- revise report parameters and run system reports as directed by the NRC;

Deleted: (e.g., resetting passwords)

Deleted: April

- investigate and resolve discrepancies in data submitted by users (e.g., when a licensee enters a source receipt for which there is no transfer);
- report to the NRC notification of lost, stolen, or recovered sources;
- log in the NRC ClearQuest change management system all reports of potential problems with the NSTS as well as any user requested changes/enhancements reported to the user support staff;
- report to the NRC and investigate all user reports of apparent inaccessibility of the NSTS;
- provide help desk support to NSTS users in all aspects of obtaining and using authentication credentials (e.g., digital certificates) and hardware token devices;
- interact with the NRC authentication credential contractor to resolve all user support requests related to these credentials or hardware tokens; and
- monitor assistance requests related to authentication credentials and hardware tokens, reporting monthly to the NRC the number and percentage of these calls that resulted in contact with the NRC authentication credential contractor.

Deleted: and

Deleted: .

Formatted: Bullets and Numbering

The Contractor shall provide and use Commercial Off-The-Shelf (COTS) help desk task tracking software. This software shall provide for reporting of support request data including: requester user group (e.g., Agreement State licensee, NRC licensee, other government agency, etc.), request reason (e.g., system use assistance, authentication credentials, or reporting a problem), and system module or function requiring explanation. The Contractor shall provide support tracking data to the NRC as requested. The data shall be in a format that can be manipulated using Microsoft Access and Crystral Reports. The Contractor shall also provide to the NRC support tracking reports on a monthly basis. The Contractor shall provide these reports with content and in a format acceptable to the NRC.

Deleted:

With regard to user support for authentication credentials and hardware tokens, the Contractor shall implement an approach that is designed to ensure that the help desk addresses 97% of all support requests of this type without escalation to the NRC authentication credential contractor. If Contractor performance falls more than 10% short of this goal (i.e., more than 13% of requests require escalation) as determined by performance in the last full month, the Contractor shall include in the monthly report a plan to address this issue and to address at least 97% of these support requests.

In the Contractor training plan for user support staff, the Contractor shall specifically address ongoing training in authentication credentials and hardware tokens. The Contractor shall identify to the NRC no more than six key support personnel to be trained in these technologies. Through the NRC authentication credential contractor, the NRC shall provide "train the trainer" training to these key support staff. This one-time training will be approximately two days in length. The Contractor shall ensure knowledge capture and a sustainable strategy to passing this training information to all appropriate user support staff.

The Contractor shall propose sufficient user support staff to provide coverage from 6:00 a.m. – 10:00 p.m. Eastern time. The Contractor shall also ensure sufficient support staff to address the anticipated surge in support needs in the first six months following NSTS V1 deployment. Should the NRC later choose to reduce the support hours, the Contractor shall reduce staffing appropriately.

Deleted: April

The Contractor shall propose and ensure availability of sufficient user support staff to provide entry of any hard copy NSTS data no later than the close of the next business day following receipt of the information.

The Contractor shall ensure that any call recorded on the user support answering system is returned within two business hours of receipt. Call returns and return attempts shall be logged in the support tracking system and associated with the initial call or message. The Contractor shall log user support phone messages such that the time of message recording is tracked.

Optional task 5.2 NSTS User Support – Option Period 1

At the option of the NRC, the Contractor shall provide all support detailed under Task 5.1, for an additional year, following the Task 5.1 performance period.

Deleted: ¶

Optional task 5.3 NSTS User Support – Option Period 2

At the option of the NRC, the Contractor shall provide all support detailed under Task 5.1, for an additional year, following the Task 5.2 performance period.

Optional task 5.4 NSTS User Support – Option Period 3

At the option of the NRC, the Contractor shall provide all support detailed under Task 5.1, for an additional year, following the Task 5.3 performance period.

6. TECHNICAL ENVIRONMENT

6.1 SafeSource Phase I Technical Architecture

The SafeSource Phase I WBL is being developed using an Oracle based Commercial Off-The-Shelf (COTS) licensing package from Versa Systems. The Versa product suite is comprised of two web-based products, LicenseEase and eGateway. LicenseEase is a full-fledged modern web-based licensing and inspection system. LicenseEase is the 'back-office' system that the internal users of the NRC will use. eGateway consists of a subset of the LicenseEase data and functionality appropriate for use by the external users of the system (e.g., the licensees, Agreement State agencies, and general public).

6.1.1 LicenseEase Architecture

The LicenseEase product is built using components from the Oracle product suite: Oracle Forms, Oracle Application Server (OAS), and Oracle Database Engine. These products are organized in a 3-tier architecture that can provide reliability, availability and scalability at each of the three tiers.

The Oracle Forms LicenseEase application is a Java 'rich' client that is deployed via the web to the NRC internal users. The client-side deployment footprint is minimal. It consists of a one-

time download of JInitiator which is Oracle's version of the Java plug-in. JInitiator automatically handles the communications / interactions between the Oracle Forms application and the Oracle Application Server which is where the bulk of the processing occurs.

The Oracle Application Server (OAS) is a Java 2 Enterprise Edition (J2EE) application server. It includes a set of services called the OracleAS Forms Services that are optimized for deploying Oracle Forms applications on the Web. The LicenseEase application logic resides on the Oracle Application Server.

The Oracle Database is a commercial relational database management system (RDBMS) that is the base upon which the LicenseEase licensing system is built. The database contains the licensing data itself and the system configuration data and business rules. The LicenseEase product implements much of its functionality using table-driven logic.

6.1.2 eGateway Architecture

The eGateway product leverages J2EE and Web Services technologies to provide an enterprise-level web "Licensing Portal" for use by external users such as licensees, Agreement State agencies, and the general public. eGateway includes a database of its own called the Enterprise Data Store. This database is used to store licensing information from one or more LicenseEase and/or other legacy licensure system implementations. It provides a way to 'roll-up' information that may be split among different departments, divisions or organizations.

eGateway is developed as a standard J2EE application (no proprietary code) that is Application Server and Database agnostic. The application logic is written as J2EE components that reside on an Orion Application Server[7]. The eGateway Enterprise Data Store is implemented using an Oracle Database instance that is separate from the LicenseEase database instance. eGateway automatically handles the interaction between the Enterprise Data Store and the LicenseEase database using a Web-Services Application Programming Interface layer provided by LicenseEase.

6.2 SafeSource Phase II Technical Architecture

It is expected that the SafeSource Phase II NSTS will be built using a multi-tiered web architecture that logically separates the three classic partitions of an information system – Presentation, Logic, and Data.

Exhibit 6-1: SafeSource Phase II Conceptual High-Level Architectural View

[7] Orion was chosen over Oracle, in this case, because Orion is more fully compliant to the J2EE standards.

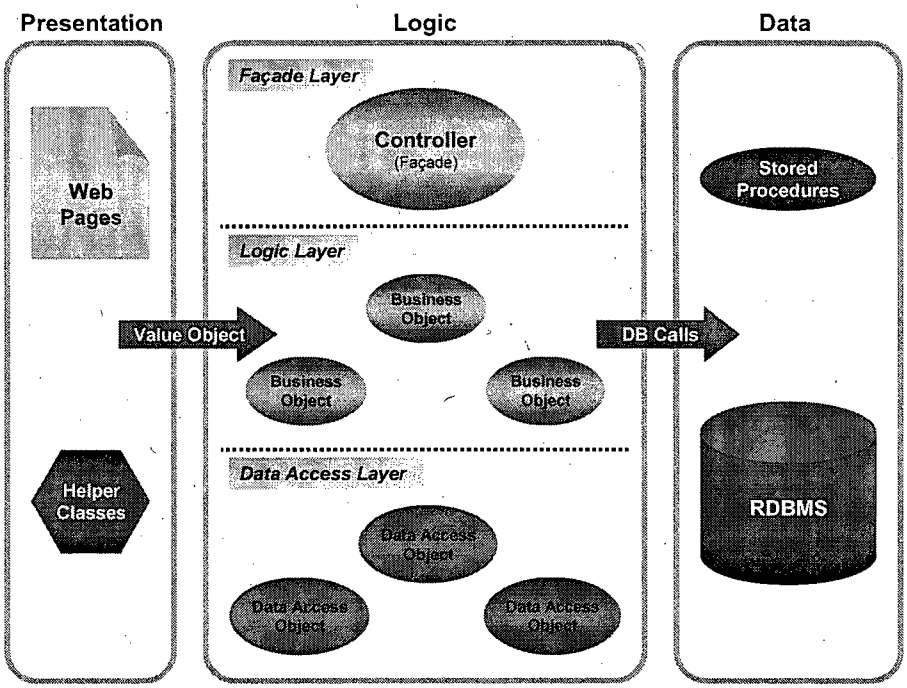


Exhibit 6-1 above shows a conceptual high-level architectural view of a properly designed multi-tiered Web application. It illustrates an information system divided into the three classic partitions – the Presentation, Logic, and Data layers. These layers ensure that each of the main architectural areas of the application remain distinct from each other. That is, each of these partitions has its own domain in which specific aspects of functionality are addressed.

- **Presentation Layer**
  The Presentation layer is comprised mainly of visual components that make up the user-interface and defines how a user interacts with the system. The user interface must be clear and concise, leveraging the best practices of visual design to create an intuitive environment for the user. The presentation layer is the one most directly responsible for Section 508 compliance.

- **Logic Layer**
  The Logic layer is where the business rules of the application reside. The business logic of the system is encapsulated in multiple well-defined discrete business objects (components) that work together under the direction of one or more controller objects which determine the order in which the business objects are called. The Logic layer also contains multiple special-purpose business objects called 'data access objects' that are responsible for actually performing operations on the data itself.

- **Data Layer**
  The Data layer is where the application's data resides. This layer is responsible for the long-term storage of data collected or generated by the system. The relational database management system's (RDBMS) data integrity and transactional capabilities are used to

ensure data integrity. This includes referential integrity features (e.g., primary key / foreign key relationship constraints) and logical unit-of-work features (e.g., atomic rollback or commit).

6.3 SafeSource Infrastructure and Operational Requirements

The NRC vision is for the NSTS to be a custom-built system that will use the same architecture established by the SafeSource Phase I project. This includes a multi-tier web architecture primarily using Oracle technologies, a commercial Application Service Provider (ASP), VPN technology, and existing LAN/WAN capabilities.

6.3.1 Multi-Tiered Infrastructure

The SafeSource infrastructure includes the following components:

- **Public firewall** – This firewall provides a gateway to the SafeSource Demilitarized Zone (DMZ). The licensees and Agreement States agencies will access the SafeSource Web Server through this firewall. This configuration will isolate the public users from the back-office system.

- **Web Server Cluster** – The web servers provide web content to licensee and Agreement State users. The web servers use the Apache web server software running on a Linux Operating System platform.

- **Internal firewall** – This firewall provides a gateway from the DMZ to the back-office systems. Access to users of the back-office systems will be granted via a secure connection and will be restricted to only users with authorized access permissions.

- **Application Server Cluster** - The application servers will use a combination of Oracle Application Server and Orion Application Server software running on a Linux Operating System platform. This offers support for J2EE, high-speed caching, rapid application development, enterprise portals, identity management, business intelligence, application and business integration, wireless capabilities, and optimized access to the Oracle database servers.

- **Database Server Cluster** - The Database Server Cluster will use the Oracle Relational Database Management System (RDBMS) and will be implemented using Oracle Real Application Clusters (RAC). Oracle RAC delivers unlimited scalability and 24x7 availability by using and managing process on all cluster nodes. In a clustered environment RAC provides for fail-over of individual session providing seamless operation during a node failure.

6.3.2 Application Service Provider

An Application Service Provider (ASP) will host the SafeSource Phase II system, as well as the SafeSource Phase I system. The ASP will provide a number of hosting services as listed below:

- It will provide and host the servers required to support the test and production environments of SafeSource Phase I and II.

- It will install and upgrade the needed operating system, database, and application software.
- It will provide server hardening and security scanning services (e.g., firewall protection, intrusion detection, etc).
- It will provide backup / recovery and offsite data storage services.
- It will provide high reliability and availability features to ensure that the system will be available as specified in the Performance Requirements section.
- It will provide access to technical support resources as specified in the Performance Requirements section.

6.3.3 Telecommunications

NRC users will access NSTS and WBL using high speed WAN and LAN connections such as those put in place between the NRC and the ASP as part of the SafeSource Phase I implementation. External users, including State Agencies, Licensees, DOE, and other Federal agencies will access the system using their local Internet connectivity. Exhibit 3-2 illustrates the telecommunication connections between the ASP, NRC, and all external users.

The Contractor shall provide a secure data communication solution that terminates at a secure location within NRC Headquarters that meets TIA/EIA-568-1 Commercial Building Telecommunications Cabling Standard Part 1: General Requirements (February 2003), TIA/EIA-568-2 Commercial Building Telecommunications Cabling Standard Part 2: Balanced Twisted-Pair Cabling Components (January 2003), and TIA/EIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces (December 2001).

The Contractor shall provide secure data communications (encryption, authentication, data integrity checking, key exchange, and data compression) commensurate with the risks inherent with communicating over public networks from the applications server located at the application service providers facility to the client computers located at NRC headquarters in Rockville, MD and DOE headquarters in Germantown, MD. The vendor proposed solution shall be constructed from components and technologies that meet or exceed National Institute of Standards and Technologies (NIST) Federal Information Processing Standards (FIPS) 140 "Security requirements for Cryptographic Modules" validation requirements.

The Contractor shall provide a secure proven Layer-2 Encryption (Layer -2 of the OSI model) data communications solution that integrates transparently into any ethernet network and supports frame authentication, dynamic per session keys, and AES 256 encryption algorithms, and has been validated as National Institute of Standards (NIST) Federal Information Processing Standard (FIPS) 140 compliant. Additionally, the vendor secure data communications solution shall be configured and operated in NIST FIPS 140 mode and meet or exceed the Department of Defense Security-Proof-of-Concept-Keystone (SPOCK) performance objectives.

The Contractor shall provide a secure client solution that support AES 256 encryption algorithms and be National Institute of Standards (NIST) Federal Information Processing

Standard (FIPS) 140 validated and shall be configured and operated in NIST FIPS 140 mode.

6.3.4 Security

Detailed information on security aspects of the SafeSource infrastructure are found in Appendix B.

6.3.5 Development Environment

The development Contractor will house the servers purchased by the NRC to provide a development environment that is comparable to the SafeSource test and production server environments.

6.3.6 Testing and Production Environments

The test and production environments will be housed in the ASP's secure and continually staffed environment, using redundant server components in a clustered environment to provide the required 99.9% system availability. The ASP facility will provide the application hosting services for the WBL and NSTS and the necessary physical and operational security features. The ASP will provide, for each system, a test environment that is comparable to the production environment.

6.4 Existing NRC Infrastructure and Operations

To facilitate effective collaboration and reduce the risk of integration problems and functional issues, Contractors should be aware of the NRC IT environment. Proposed technical approaches must be compatible with the prevailing NRC environment at the time of proposal submission and must ensure compatibility with any anticipated changes expressed within this document.

Compatibility concerns differ during the development process (including definition, design, and testing) and at the time of production deployment. While not comprehensive, the following sections will describe significant factors related to IT infrastructure compatibility during all project phases. The Contractor must submit any environmental compatibility questions to the NRC Contracting Officer prior to the deadline for submission of proposals.

6.4.1 Compatibility During Development

This section summarizes IT environment concerns relating to definition (e.g., requirements validation), design, development, and testing activities.

While the Contractor may need to perform some work on the NRC campus, the NRC expects most SafeSource Phase II project work will be performed remotely, at Contractor offices. The NRC expects that frequent collaboration will be done through broadband connections to the NRC network. The prevailing method of connection uses Citrix Metaframe servers. This will require installation of a client module on each Contractor workstation accessing the NRC network. The NRC is also pursuing limited use of Virtual Private Network (VPN) connections for intense remote database applications. The proposed technical approach shall utilize VPN connectivity, configured to meet the NRC and DOE security requirements

The prevailing NRC desktop environment consists of Windows XP professional edition, Groupwise v6.x email, Internet Explorer, and the Corel office suite. NRC staff working directly

on this project will also use the Microsoft Office suite (Word, Excel, Powerpoint, and Access) as well as Microsoft Project and Visio. It is also notable that the Rational Suite Enterprise will also be used extensively on this project, by both Contractor and NRC personnel.

The Contractor shall prepare all project documents using the prevailing version of Microsoft Office suite, Microsoft Project, or Rational products, as directed by the NRC Project Manager. At the discretion of the NRC, the Contractor shall deliver products in the format compatible with Microsoft products up to two versions older than the prevailing version.

The Contractor shall fully use the Rational Suite Enterprise as directed by the NRC Project Manager. In particular, the following Rational point products are used:

- **Requisite Pro** Used for requirements definition and management, largely based on use cases and Unified Modeling Language (UML) diagrams
- **Rose** UML modeling tool - to be used for use case refinement and all Contractor design activities.
- **ClearQuest** Used for change management - to be used by the Contractor and the NRC to log and track all change requests after requirement validation and baseline establishment and to log and track all requirement changes discovered during requirement validation efforts
- **TestManager** To be used by the Contractor to define test plans, test cases, and to indicate the relation of test cases to test scripts and requirements
- **Robot and ManualTest** To be used by the Contractor to implement each test case as either an automated test (preferred by the NRC where practical – required for system testing) or electronically managed manual test script
- **SoDA** The primary reporting tool within the Rational suite. The Contractor will use this to produce both standard and customized reports as required on this project.
- **ClearCase** To be used for all Contractor CM activities throughout the project
- **ProjectConsole** Used by the NRC for earned value reporting and general project information dissemination

6.4.2 Compatibility In Production Deployment

The NSTS shall use a Web-based, three tier architecture, hosted at an ASP site. While the Contractor may propose any approach to the presentation layer (user interface), the NSTS shall use the Oracle database engine and Oracle application server. The Contractor shall ensure that the NSTS hosting environment is compatible with the WBL system and that the two systems can share servers and other hardware and software customarily provided by an ASP. The Contractor shall also ensure compatibility with any other systems where data sharing or interfaces are specified within the NSTS requirements.

6.5 Government Furnished Equipment

The NRC will be responsible for the following resources related to performance of work described within this PBSOW:

- providing support needed within the NRC and DOE to cooperate with Contractor efforts to establish connectivity to Contractor and Application Service Provider sites;
- Providing Contractor access for installing any client components of the NSTS software on NRC desktops;
- providing space at NRC sites to conduct NSTS training sessions for NRC staff (the Contractor shall propose costs for hosting licensee workshops and training sessions);
- Providing broadband access to Rational Suite licenses (limited to use of RequisitePro, Rose, ClearQuest, and SoDA).; and
- Providing licenses to Rational TestManager, Robot, ManualTest, RequisitePro, and Rose for use at the Contractor site.

The Contractor shall provide all necessary information (e.g., hosting site communications specifications, communications line capacity requirements, desktop software installation procedures, and training room requirements) and support that is requested by the NRC in order to furnish these resources for activities to be conducted within NRC facilities.

The Contractor shall provide and pay recurring costs for all leased lines or telecommunications infrastructure (e.g., VPN appliances) required to connect NRC and DOE facilities to the ASP or other sites included in the SafeSource infrastructure, including any dedicated lines or telecommunications infrastructure required for user support and software maintenance activities.

Development servers and any additional software required will also be considered "government furnished equipment" even though the NRC will authorize the Contractor to procure such hardware and software components on behalf of the government. The NRC further expects that the operational support task ASP support will provide leasing of licenses for the Oracle database and application server software. However, if the proposed technical approach requires NRC purchase of any Oracle product licenses, the Contract shall explicitly state this and include detailed product specifications with the proposal.

The NRC will tag and maintain property control of this equipment and the Contractor is expected to notify the government within 48 hours after any equipment is received at the Contractor's site or moved to another facility so that government staff can conduct inventory control, tracking, and monitoring activities. In addition, the Contractor shall notify the government within 24 hours if the equipment is lost or sustains damage.

The Contractor shall provide detailed specifications on any Oracle software products required to support their technical approach. The NRC is specifically required to procure all Oracle products through a government wide program. After procurement, these products would be provided to the Contractor for use on the SafeSource Phase II project.

6.6 Compliance with the NRC System Development Methodology

The NRC is implementing a new Project Management Methodology (PMM), replacing the previous System Development Life Cycle Management Methodology (SDLCMM). The Contractor shall propose sufficient resources to comply with the PMM. For Contractor reference, software development aspects of the PMM are based on the Rational Unified Process (RUP). PMM templates for significant Contractor products are attached to this document as appendices.

All Contractor proposals must demonstrate dedicated project staff with expertise and experience in the use of RUP and the Rational Suite Enterprise.

In support of PMM, the Contractor shall use the Rational tools specified in Section 6.4.1 as well as other Rational suite tools that the Contractor deems helpful in improving efficiency and effectiveness in performing NSTS work. All PMM documentation available at the time of this solicitation will be included in appendices cited in each deliverable description. The Contractor shall contact the NRC Contracting Officer with any further questions, prior to the deadline for proposal submission.

7. DESIGN AND IMPLEMENTATION CONTROLS

7.1 General Design and Implementation Controls

During the detailed design phase of the project, the Contractor shall adhere to the PMM. The Contractor shall take direction on any methodology interpretation solely from the NRC Project Manager.

The Contractor shall use the Rational Suite Enterprise which is currently used by the NRC to support and manage all phases of software development.

The Contractor shall establish a configuration management (CM) capability (e.g., software/ procedures) capable of managing both project documents and software assets throughout the project. Within the Configuration Management Plan, the Contractor shall propose an approach for interfacing and synchronizing with the central NRC CM repository, maintained using Rational ClearCase. This approach must address the need for the NRC IV&V team to dynamically review Contractor products throughout the project. The Contractor shall also provide any support needed by NRC CM staff in reviewing and processing deliverables.

The Contractor shall propose sufficient resources to support hosting a ClearCase server at the Contractor facility. The Contractor shall propose the effort to host this server and to synchronize with the central NRC CM server as often as directed by the NRC. This synchronization may be accomplished through transmittal of electronic media (e.g., CD/DVD) or by electronic transfer of necessary files. The Contractor shall provide an optional pre-costed plan for active replication of the NSTS ClearCase repository between the Contractor ClearCase server and the central NRC CM server.

7.2 Detailed Design and Implementation Controls for Security

NRC Management Directives (MD), Office of Management and Budget (OMB) Circulars, National Institute of Standards and Technology (NIST) Special Publications, the Federal Information Security Management Act of 2002 (FISMA) and other federal publications and laws,

outline specific requirements and guidance for ensuring that system security controls are included in the design of a system such as the NSTS. The NSTS is classified by the NRC as a "Major Application". (See References at §7.2.7)

The Contractor's proposal shall anticipate the full range of security and access control features needed with regard to the potential user communities and functions described in the functional requirements.

The Contractor shall provide identification and authentication controls, auditing controls, access controls, secure systems administration capabilities, system backup capabilities, and the capability to reliably recover in the event of a component failure among the security components that the NRC requires. The NRC also requires that the Contractor shall develop the appropriate security documentation for the NSTS to ensure compliance with current federal guidelines (see References at §7.2.7). These guidelines require that the following items be developed: a System Security Risk Assessment, a System Security Plan (SSP), an IT Contingency Plan, IT Contingency Plan training, IT Contingency Plan testing, an IT Contingency Plan Test Report, a System Certification and Accreditation Report, and a Security Self-Assessment. The Contractor shall also support the NRC in the accomplishment of a disaster recovery test of the system, which will validate the backup and recovery capabilities defined in the Contingency Plan. Major deficiencies and vulnerabilities that are identified during any of the system or security testing or during the system certification process shall be corrected and/or mitigated by the Contractor.

Identification and Authentication
The NRC anticipates multiple classes of NSTS users who are afforded access to differing levels of detailed information based upon identity and authority (roles). Authentication focuses on confirming a person's identity, based on the reliability of his or her credential. OMB E-Authentication Guidance and NIST SP 800-63 *Electronic Authentication Guideline* provide instruction on how to implement e-authentication by assessing risk and determining the appropriate level of required identify assurance.

The Contractor shall conduct and document a risk assessment with specific attention to authentication, following the OMB guidance that will identify risks, map those risks to the required assurance level, and recommend an authentication technology solution appropriate for attaining the required assurance level. The proposed solution shall provide appropriate Identification and Authentication controls, described in NRC Management Directive (MD) 12.5, for each class of user. Upon implementation the Contractor shall have user identification and authentication controls in place to ensure only authorized (registered) persons (or processes) are able to obtain access and only to the levels authorized. Specifics on classes of users will be defined after contract award.

Auditing Control
The Contractor shall ensure that controls, described in NRC MD 12.5, which specifically monitor or allow auditing of system activity are in place and implemented. These controls will record events such as: user logon attempts; attempts to access data or perform functions for which the user is not authorized; changes to the system security configuration; changes to a user's privileges; creation or deletion of accounts, records or data; etc. These audited events must be logged and available for routine periodic review. Automated rules shall be available to issue administrator alerts when particular unauthorized activities occur.

Discretionary Access Control

The NSTS shall provide NRC systems administrators the capability to qualify the access privileges of each user ensuring that authenticated, registered users can only access data and perform operations for which they have been authorized. Specifics on access authority will be defined after contract award.

Secure Web-based Administration
The NRC anticipates that the proposed application will reside on servers housed at a location remote to the NRC which is maintained by a commercial ASP. Understanding that some application and system administration functions will be the responsibility of the system owner (NRC), the Contractor shall propose a means for NRC to securely access the application. Identification and Authentication controls, Auditing and Access controls shall apply. The Contractor shall propose connectivity for this purpose via a high speed, secure link and be prepared to provide and implement a communication capability managed by a government approved security software solution (for example, SSH).

Per NRC MD 12.5, written management authorization shall be obtained from the OIS before establishing a connection between the NRC IT infrastructure and any other system that is not NRC controlled. Depending upon the Contractor's proposed solution such authorization may be necessary before any connection can be established.

System Backup and Recovery
The Contractor shall deliver a reliable and comprehensive solution to ensure easy and rapid recovery of NSTS functionality in the event of component failure. The solution shall include a comprehensive backup and recovery capability. The Contractor shall also support the NRC in the accomplishment of a disaster recovery test of the system, which shall validate the backup and recovery capabilities.

Other Security Considerations and Requirements
The Contractor shall propose a methodology for handling and tracking damaged media or decommissioned equipment to ensure the integrity of any information that may have been contained or processed by the media or equipment.

Implementation of the NSTS shall include an appropriate Warning Banner, a User Responsibilities (Terms and Conditions) link and a Privacy Policy link. NRC will work with the Contractor to develop the content for these items.

All NSTS source code and Contractor-developed modules shall be the sole property of the NRC. Within the proposed development approach, the Contractor shall clearly identify any proposed proprietary software libraries, modules, sub-systems, or off-the-shelf products that will be used in development or operational use of the NSTS. For any such products, the Contractor proposal shall include the intent to transfer use rights to the NRC or shall include the cost to the NRC for obtaining licenses as part of the NSTS government furnished equipment.

References

Computer Security Act of 1987;
(**http://www.cio.gov/archive/computer_security_act_jan_1998.html**)

Department of Commerce (DOC) Abbreviated Certification Methodology Worksheets 1 through 6; (**http://csrc.nist.gov/publications/secpubs/doc-cert.txt**)

Federal Information Processing Standards Publication (FIPS PUB) 102, Guidelines for Computer Security Certification and Accreditation.

FIPS PUB 140-2, Security Requirements for Cryptographic Modules;

FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems;

Federal Information Security Management Act of 2002 (FISMA), (**http://csrc.nist.gov/policies/HR2458-final.pdf**)

General Accounting Office (GAO) Federal Information Systems Control Audit Methodology (FISCAM), (**http://www.gao.gov/special.pubs/ai12.19.6.pdf**)

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, "Guide for Developing Security Plans for Information Technology Systems.; (all NIST Special Pubs are available at **http://csrc.nist.gov/publications/nistpubs/index.html**)

NIST SP 800-26, Security Self-assessment Guide for Information Technology Systems.;

NIST SP 800-30, Risk Management Guide for Information Technology Systems.;

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.;

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Technology Systems.

NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.;

NIST SP 800-53, Recommended Security Controls for Federal Information Systems;

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I and Volume II;

NIST SP 800-63, Electronic Authentication Guideline;

NRC Management Directive (MD) 12.1, NRC Facility Security Program;

NRC MD 12.2, Classified Information Security Program.;

NRC MD 12.3, NRC Personnel Security Program;

NRC MD 12.4, Telecommunications Systems Security Program.;

NRC MD 12.5, Automated Information Security Program.;

NRC MD 12.6, Sensitive Unclassified Information Security Program.;

Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources; (**http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf**)

OMB E-Authentication Guidance;
(**http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf**)

7.3 Detailed Controls for Engineering, Development, and Testing

The Rational Suite Enterprise is currently used by the NRC to support and manage all phases of software development. Key Rational Suite products used by the NRC are:

- Rational Rose - creation and management of Unified Modeling Language (UML);
- RequisitePro - requirements management;
- ClearQuest - change management and defect tracking;
- ClearCase - configuration management;
- Test Manager, Robot and ManualTest - functional testing and test log management;
- SoDA - integrated reporting;
- Crystal Reports (V10) for extended reporting capabilities; and
- ProjectConsole.

The SafeSource Phase II project will use a Configuration Control Board (CCB) beginning in the design phase. This group will have representatives from the system business sponsor as well as NRC information technology specialists.

The NRC uses central configuration management (CM) for all systems under development or maintenance. This function is currently supported by Rational ClearCase with replicated servers.

The NRC maintains a Consolidated Testing Facility (CTF). On the SafeSource Phase II project this facility will be used for integration testing, acceptance testing and demonstrations, as determined by the NRC Project Manager.

The Contractor shall:

- perform software and system engineering required to address and comply with all documented NRC requirements and specifications;
- deliver pre-production release versions of all system builds and deployment packages until the conditions of the NRC Acceptance Test Plan are satisfied;
- support and be responsive to an Independent Verification & Validation (IV&V) Contractor in its assessment of requirements compliance, design review, product testing and evaluation;
- utilize the Rational Suite Enterprise point products as required by the NRC Project Manager and in compliance with the prevailing NRC PMM;

- provide to all Contractor staff training required to ensure effective use of all Rational Suite products that the Contractor is to use, as directed by the NRC project manager;
- document in Rational ClearQuest all requirement revisions proposed during the requirements validation process;
- support an NRC-provided server that will host the Contractor-site replicated NSTS ClearCase database and provide capable staff to manage the server and ClearCase database;
- provide a connectivity strategy, acceptable to the NRC, for supporting ClearCase replication;
- provide support, as needed, for NRC testing within the CTF;
- host at the Contractor's facility all testing that the NRC chooses not to perform within the CTF; and
- provide all required system documentation.

7.4 Engineering the Solution

During the software engineering phase of each SafeSource task, the Contractor shall refine and continuously update and maintain a Software Development Plan (SDP). The SDP will detail the activities and schedules for designing, coding, integrating, and testing for each module of the NSTS. Any design updates or changes require approval from the NSTS CCB.

The Contractor shall provide briefings to the CCB as needed for presentation of recommended design specifications or changes. In requesting concurrence with design specifications or permission for changes, the Contractor shall address impacts to the system, in terms of changes to the schedule, operational effectiveness, and maintainability. The Contractor shall also provide detailed descriptive materials for NRC review when proposing any design specifications or changes (e.g., UML diagrams and screen prototypes).

Based on the updated SDP, the design documents, and the results of the walk through sessions, the Contractor shall design the system engineering solution that integrates the operational capabilities. The preferable engineering solution will:

- utilize the Oracle database and application server; and
- employ object oriented development process and tools for the presentation layer. The Contractor shall provide detailed information on all Contractor in-house methodologies and standards to be employed during development and integration of the proposed solution, documenting how these will support and not conflict with the NRC PMM and RUP.

Throughout the process of design refinement, the Contractor shall perform revisions to the Rational Rose detailed design model as often as directed by the NRC Project Manager. The intent is that the design model will always be current within a margin of three business days.

Additionally, the Contractor shall revise the SDP or otherwise provide documentation of system engineering decisions in a format acceptable to the NRC Project Manager. The NRC goal is that all design decisions be documented within the Rational Rose detailed design model, using descriptive text where needed. As the primary outputs of this phase, the Contractor shall deliver:

- a detailed design model that will be developed and maintained by the Contractor for NRC review as requested by the NRC; and
- comprehensive documentation, in Rational RequisitePro, ClearQuest, and Rose, of all design specifications and clarifications to NRC requirements identified during this task.

Development
Using the design materials noted above, the Contractor shall establish a system that satisfies the design specifications.

The Contractor shall be responsible for all activities associated with system development including, but not limited to, building the database structures, associated tables, validation routines, data dictionaries, and software units. The Contractor shall be responsible for all integration activities including, but not limited to, the integration of software units into software modules, integrating modules into subsystems and systems, and integrating those systems.

Unit and Integration Testing (White Box Testing)
In responding to this solicitation, the Contractor shall provide detailed descriptive information on their methodology for unit and integration testing. This descriptive information shall describe but not be limited to how the proposed methodology ensures independence of testing from development personnel and activities. Any automated testing shall be conducted using the Rational Robot and Test Manager tools and all scripts and test logs shall be delivered to the NRC upon request from the NRC Project Manager. With approval from the NRC Project Manager, the Contractor may use the Rational ManualTest tool to develop scripts where automated testing is deemed impractical. Testing shall be performed by the Contractor following an established software quality assurance methodology of the Contractor's choosing, contingent on NRC's approval of the recommended methodology. The government may audit tests as part of its own Test and Acceptance Program.

Working with the NRC to obtain necessary example data, the Contractor shall develop a standard test dataset for use in all levels of NSTS testing. The Contractor shall also deliver and maintain under NRC central CM all scripts needed to create and refresh the testing database.

The output products and deliverables of this task are unit and integration test plans, related test result reports, and scripts for creation and refreshing of the standard testing database. The Contractor shall ensure that all test plans, test logs, and test result reports are entered into the project CM library for transmittal to the NRC CM repository as directed.

System Testing (Black Box Testing)
The Contractor shall develop draft and final versions of the NSTS System Test Plan (STP) for each production system build. In these comprehensive plans, the Contractor shall provide explicit test cases for demonstration of the correct and complete fulfillment of all requirements and design specifications. In addition to common user functions, the STP shall address testing of operational functions such as the backup and recovery capabilities under at least two

scenarios: a partial recovery and a complete rebuild/recovery. The Contractor shall ensure that the STP is developed and organized from the perspective of each Actor described in the requirements use cases. Development of the STP will require integration between Rational RequisitePro, Rose, and TestManager.

The Contractor shall implement each STP as a Rational TestManager test plan, TestManager test cases, and a suite of scripts using Rational Robot and ManualTest (if approved). Any Robot scripts created by the Contractor shall comply with the NMSS functional testing standards found in Appendix R. If the Contractor does not have access to the necessary Rational software, the Contractor shall arrange to have staff perform test script development work at NRC Headquarters. At the discretion of the NRC Project Manager, the NRC may provide Rational testing software for use at the Contractor site.

The Contractor shall demonstrate full use of STP test cases and scripts. The Contractor shall provide both draft and final deliveries of the STP, with time allowed for NRC review and comment. In the final draft, the Contractor shall address all draft comments to the satisfaction of the NRC project manager.

During the Development Phase, the Contractor shall implement the STP. The government will audit these tests as part of its own test and acceptance program. Testing should be iterative with scheduled Pre-final and Final Testing. The purpose of these two separate test periods is to allow time for the Contractor to make corrections identified during the Pre-final Test and incorporate all necessary changes prior to completing the Final Testing. The Contractor shall run the entire system test suite against each new system build that is created.

The NRC will subject the completed system to its acceptance test process prior to accepting delivery of the product. All hardware and software components will be tested against the defined functional requirements and design specifications. The government will implement detailed code review against developed code, scripts, CGIs, etc. The detailed code review will not be routinely performed against the "out-of-the-box" functionality of packaged software (operating system, RDBMS, etc.) unless customization (previously identified by the Contractor and approved by the government at the design review) is performed by the Contractor on the software packages.

The Certification and Accreditation Report, referenced in Section 7.2 of this document, must result in at least an interim accreditation before the system will be accepted. NRC MD 12.5 provides guidelines for accomplishing the Certification and Accreditation.

After NRC Pre-final acceptance testing has been completed and required changes have been addressed by the Contractor and sufficiently tested in the Final Test, the Contractor shall conduct a readiness review session with NRC and present the results of all activities, findings, and products developed during the engineering phase. The Readiness Review Demonstration shall be scheduled immediately upon completion of the Engineering phase. The Readiness Review Demonstration shall group topics as logically as possible to facilitate comprehensive yet succinct issue coverage, as this will be the first major checkpoint in the system development life cycle. Based on a successful review, NRC will issue a go/no go decision on deployment of the National Source Tracking System.

Contractor's Test Report

For each system module, the Contractor shall develop and deliver a Test Evaluation Summary (TES), following the PMM template in Appendix O. While the NRC reserves the right to review

all Contractor unit and integration testing reports, the Contractor shall deliver a TES for the final unit and integration testing of each build. The Contractor shall deliver a separate TES regarding the system testing of each build. For the system testing and any other testing using automated tools, the Contractor shall deliver the electronic test log files and script databases and include hard copy of these logs, including verification point comparator screen images, in the TES. The Contractor shall also include in the TES sections covering test result analysis, remediation, work-arounds, unresolved issues, and enhancements recommended for future releases. The Contractor shall also enter into ClearQuest any unresolved issues and recommended enhancements.

The output products and deliverables of this task are fully tested software modules and subsystems which are stored in the NRC central CM library, including the TES, and electronic files containing all test scripts and logs.

7.5 Detailed Controls for Training

Training Plan
The Contractor shall develop and implement comprehensive training and support plans that address all user roles relating to the software products provided under the task. Specifically, the Contractor plan should address the training needs of the following user groups:

- external users such as Licensees and Agreement State personnel, who will enter NSTS data;
- other external users who might be permitted to query the database through a web interface;
- NRC and DOE users who will analyze source tracking transactions, alerts, and discrepancies; and
- NRC users who will perform administration and configuration of the NSTS.

The Contractor shall grant to the NRC exclusive and unlimited rights to copy and distribute all training materials including CBT modules.

The Contractor shall ensure that all files and program code related to training modules are maintained using the same configuration management guidance described for system artifacts.

The deliverables related to training are:

- draft and final versions of the National Source Tracking System Training Plans;
- electronic versions of all training materials for use in the hands-on training sessions (including the guide for formatting and submission of electronic data files); and
- all files and program code and materials related to CBT, both portable (CD/DVD) and web-based training modules.

On-Line Help System and Tutorials
The Contractor shall:

- ensure that all modules of the NSTS have online help available through a consistent interface;
- provide all support needed to add NRC-specific information to online help screens; and
- ensure that all online help files and program code are maintained using the same configuration management guidance described for system artifacts.

7.6 Detailed Controls for Ongoing Support

The Contractor shall be responsible for providing ongoing support for NSTS V1 after it becomes operational and for the enhanced system (NSTS V2) after it becomes operational. Activities shall include:

- refreshing all servers at least every two years, with models that employ current technology;
- providing access to and support for DBMS and any licensing of other system modules;
- providing continuous infrastructure services (server hosting, dedicated and Internet connectivity, backup and recovery, intrusion detection etc.);
- providing data base administration services; and
- providing training as needed to ensure that NRC personnel and licensees can effectively use new releases of the NSTS.

8. ORDER TERMS, CONDITIONS, AND REQUIREMENTS

8.1 Performance Requirements

The deliverables required under this order must conform to the standards contained, or referenced, in the performance based statement of work. All deliverables required under this order must be delivered to the NRC in electronic format (Word) and ADOBE Acrobat Portable Document Format (PDF). At the same time, the Contractor shall provide 3 printed copies of each deliverable, and any Rational Suite files, if applicable. The Contractor shall deliver draft versions of all deliverables required under this order.

8.2 Place of Performance

Place of performance shall be primarily at the Contractor site(s) for all tasks. Contractor staff shall be required to be at the NRC Headquarters offices during each task to conduct interviews, deliver presentations, and attend status meetings, as well as any and all other NRC-specific activities that occur during the period of performance. Training requires that the Contractor travel to Regional offices and the Organization of Agreement States meeting to conduct 12 training sessions; seven of these training sessions are during performance of Task 1 and the remaining five training sessions are expected to occur during performance of Optional Task 2. The Contractor shall also travel to licensee workshops. In addition, the Contractor may be required to work at the NRC on an intermittent basis when conducting Integration tests at the NRC's Consolidated Test Facility. Should the Contractor require access to DOE facilities, the NRC will provide a DOE contact person to assist in the necessary clearance process.

8.3 Travel

Travel includes Local Travel as well as travel to other parts of the U.S. to conduct workshop sessions, presentations, and training. For planning purposes, the contractor shall use an estimated travel cost of $64,000 for Task 1 and $12,000 for Task 2.

8.4 Reporting Requirements

8.5.1 Weekly Reports and Meetings

The Contractor shall provide weekly Activity Reports to include any exceptions or changes from the existing plans. The weekly report will be delivered by close of business each Tuesday. The weekly report will include a proposed agenda for the meeting to cover management issues and any technical issues that would impact schedule, cost, or technical risk.

8.5.2 Project Management Plan

The Contractor shall submit a detailed Project Management Plan to cover Tasks 3, 4, and 5. For Tasks 1 and 2, the Software Development Plan will serve as the Contractor project management plan. Further references to Project Management Plan shall also apply to Software Development Plans. The plans will show tasking and sub-tasking, milestones, labor categories and/or staff assigned and the projected number of hours estimated to complete each task/subtask by staff member. For each task, the Contractor shall maintain a schedule in Microsoft Project® format, with detailed data sufficient to meet the earned value reporting requirements described in Appendix S. In addition, the Contractor shall ensure that the WBS, as represented in Microsoft Project is decomposed to a sufficiently detailed level such that no task (work package) requires more than 80 or fewer than eight staff hours. Each plan and schedule will be maintained at the above level of detail on a monthly basis for the duration of the task. Each Project Management Plan will also include dollars by labor category/assigned personnel which will support the Contractor's estimate for each task executed under this contract. The Contractor shall maintain all Microsoft Project schedules and any other files needed for earned value reporting in a shared space such that the NRC may access these at any time. The contractor shall ensure that all Microsoft Project files are updated within two business days of any change. The Contractor shall ensure that all Microsoft Project schedules and associated Software Development or Project Plan documents remain synchronized with changes applied to the Microsoft Project files within two business days of NRC approval.

8.5.3 Monthly Reports and Meetings

The Contractor shall provide a Monthly Status Report to the NRC Project Officer and the Contracting Officer by the 15th of each month. Each monthly report will include updates to the Project Management Plan and schedule (Work Breakdown Schedule), listing the reasons for changes, proposed adjustments and justification, cost and schedule impacts.

The Contractor shall maintain each Project Management Plan with the latest hours/costs and submitted as part of the monthly report. All phases and tasks in the Work Breakdown Schedule must be updated with % completion statistics at a sufficient level to allow the Contractor to report the "Earned Value" Statistics for the overall project. If at any time the project deviates from 5% in cost or schedule from the project management plan, the Contractor shall schedule an update with the NRC Project Manager immediately.

The report shall also contain the BPA number, order number, and task; the period covered by the report; a summary of work performed during the reporting period for each task, including appropriate statistics and plans for the next reporting period; a discussion of project plans, hardware problems, current operational problems, and the proposed corrective action, and

analysis of the impact on other tasks within the scope of the PBSOW; and a status of expenditures under the order for the reporting period, cumulative expenditures to date, funds obligated to date, and balance of funds required to complete the order; any project risks and appropriate risk mitigation strategies especially those which require NRC management action; and a list of any deliverables completed during the prior month as well as deliverables scheduled for completion during the next month and the schedule and cost variances, if any, for those upcoming deliverables.

The Contractor shall attend a monthly status meeting in conjunction with the next regularly-scheduled weekly meeting and review the project status for the prior month.

8.5.4 Provide Data for Earned Value Reporting

The Contractor shall track project tasks, milestones, and resources in Microsoft Project, performing at least weekly updates to the Microsoft Project data. The Contractor shall ensure that the Microsoft Project files are set up to support NRC Earned Value (EV) reporting. The Contractor shall provide EV data to the NRC monthly, on a schedule acceptable to the NRC Project Manager. The Contractor shall ensure that all EV tracking and data deliveries comply with the Earned Value Reporting Technical Guide attached in Appendix S. The Contractor shall maintain Microsoft Project data in a shared location, accessible by appropriate NRC personnel and IV&V contractors. Additionally, the contractor shall ensure that each WBS, as represented in Microsoft Project is decomposed to a sufficiently detailed level such that no task (work package) requires more than 80 or fewer than eight staff hours.