

NRC DR 07 09 136

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES
1 2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

BPA NO.

1. DATE OF ORDER 03-05-2009
2. CONTRACT NO. (if any) GS35F0376N
3. ORDER NO. MODIFICATION NO. 4. REQUISITION/REFERENCE NO. NSR-09-136
5. ISSUING OFFICE (Address correspondence to) U.S. Nuclear Regulatory Commission
6. SHIP TO: a. NAME OF CONSIGNEE U.S. Nuclear Regulatory Commission
b. STREET ADDRESS Office of Nuclear Sec. & Inc. Response
7. TO:
8. TYPE OF ORDER a. PURCHASE b. DELIVERY
9. ACCOUNTING AND APPROPRIATION DATA 911-15-5D1-133 I1119 2572 31X0200.911
10. REQUISITIONING OFFICE NSR Nuclear Security and Incident Response

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
a. SMALL b. OTHER THAN SMALL c. DISADVANTAGED d. WOMEN-OWNED e. HUBZone f. EMERGING SMALLBUSINESS g. SERVICE-DISABLED VETERAN-OWNED
12. F.O.B. POINT N/A
13. PLACE OF a. INSPECTION b. ACCEPTANCE
14. GOVERNMENT B/L NO.
15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)
16. DISCOUNT TERMS NET 30

Table with 7 columns: ITEM NO., SUPPLIES OR SERVICES, QUANTITY ORDERED, UNIT, UNIT PRICE, AMOUNT, QUANTITY ACCEPTED. Row 1: The Contractor shall provide 'SAFEGUARDS INFORMATION LOCAL AREA NETWORK & ELECTRONIC SAFE (SLES) OPERATION AND MAINTENANCE (O&M)' Services IAW the terms and conditions of its GSA contract...

18. SHIPPING POINT
19. GROSS SHIPPING WEIGHT
20. INVOICE NO.
21. MAIL INVOICE TO: a. NAME Departement of Interior National Business Center
b. STREET ADDRESS (or P.O. Box) Attn: Fiscal Services Branch - D2770 7301 West Mansfield Avenue
c. CITY Denver d. STATE CO e. ZIP CODE 80235-2230
17(h) TOTAL (Cont. pages)
17(i). GRAND TOTAL
OBLIGATED: \$300,000.00

22. UNITED STATES OF AMERICA BY (Signature)
23. NAME (Typed) Heriberto Colón, Jr. Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER Page 1

AUTHORIZED FOR LOCAL REPRODUCTION PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 4/2006) PRESCRIBED BY GSA/FAR 48 CFR 53.213(f)

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

MAR 25 2009

ADM002

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 03-05-2009	CONTRACT NO. GS35F0376N	ORDER NO. NRC-DR-07-09-136
-----------------------------	----------------------------	-------------------------------

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
<p><b>ACCEPTED:</b></p> <p>PRINT NAME &amp; TITLE Michelle Jafari, VP Operations</p> <p>SIGNATURE <i>Michelle Jafari</i> DATE 3/5/09</p>						

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))



**U.S. NUCLEAR REGULATORY COMMISSION (NRC)  
OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE (NSIR)**

## **STATEMENT OF WORK**

**Safeguards Local Area Network and Electronic Safe (SLES)  
Operations and Maintenance**

**NRC-07-09-136 - Enclosure 1 – SOW**

1	Background .....	3
2	System Overview .....	4
3	Objective .....	5
4	Scope of Work .....	5
5	General Requirements .....	6
6	Tasks .....	8
6.1	<i>Transition SLES to Operate Under a New Support Agreement</i> .....	8
6.1.1	Kick-off meeting .....	8
6.1.2	Operating plan .....	9
6.2	<i>System Administration</i> .....	9
6.2.1	System Performance Monitoring .....	9
6.2.2	System Backup .....	10
6.2.3	System Recovery .....	10
6.2.4	Client Terminal Image Backup .....	11
6.2.5	Database Administration .....	11
6.2.6	Portal Administration .....	12
6.2.7	(Optional) Records/Documents (Documentum) Administration .....	12
6.3	<i>User Support</i> .....	12
6.3.1	Users Registration and Access Authorization Management .....	12
6.3.2	Help Desk and User Desktop Support .....	12
6.3.3	(Optional) Record / Document Management and User Desktop Support .....	14
6.3.4	Kiosks Administration and support .....	14
6.4	<i>System Maintenance</i> .....	14
6.4.1	Daily Activities .....	16
6.4.2	Weekly Activities .....	17
6.4.3	Monthly Activities .....	17
6.5	<i>Server Shutdown and Restart</i> .....	18
6.6	<i>Disaster Recovery</i> .....	18
6.7	<i>Configuration Management</i> .....	18
6.8	<i>System Documentation Reference and Update</i> .....	19
6.9	<i>Transition SLES Operations and Maintenance to OIS</i> .....	19
6.9.1	Transition meeting(s) .....	19
6.9.2	Update the Operating plan .....	20
7	Status Meetings and Progress Reporting .....	20
8	Procurement Responsibilities .....	21
9	Contractor Personnel Skill Set Requirements .....	21
10	Protection of Proprietary Information .....	23
11	System Security and Requirements for Handling SGI .....	23
12	Travel .....	25

## 1 Background

The Nuclear Regulatory Commission (NRC) mission is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment.

The NRC generates and maintains electronic and paper copies of sensitive unclassified documents that contain Safeguards Information (SGI). SGI is information about the sensitive security concerns related to the physical protection of special nuclear material, source material, byproduct material, and nuclear power plant facilities. SGI information is generated and maintained by authorized custodians in several NRC offices using secure safes to control and ensure protection from unauthorized disclosures. Most of the SGI documents are in paper form, and are stored in lock-bar cabinets. There are also some electronic files stored on CDs and removable hard disks which are also kept within the lock-bar cabinets. Over time, managing SGI paper copies, individual CDs, and files on removable hard disks in the secure lock-bar safes has become increasingly difficult and caused delays in locating, accessing, and sharing SGI information with authorized staff. There have been problems in quickly searching, locating, and communicating with Licensees and other Federal, Local, and State governments that are responding to time-critical events involving SGI concerns.

The NRC is developing and implementing a secure intranet capability that allows authorized NRC staff in the Headquarters and the Regional Offices to share SGI information in a secure and effective manner. The NRC will be extending this secure capability to external users authorized for handling SGI at Licensee, Federal, Local, and State government organizations. The need for federal and state agencies to share sensitive information and coordinate in mitigating risks from nuclear incidents has formed the basis for requirements to provide an integrated solution that works seamlessly with other agency functions and interagency communication initiatives.

The scope of this procurement is limited to operation and maintenance of the Safeguards Local Area Network and Electronic Safe (SLES) which provides a secure intranet capability allowing appropriate NRC staff to share Safeguards Information (SGI).

SLES consists of two distinct parts, the Safeguards Local Area Network (SGI LAN) and the Electronic Safe (E-Safe). SGI LAN is the supporting infrastructure and E-Safe is the application that resides on the SGI LAN; which provides electronic records/document management of agency SGI.

NSIR adopted a phased approach for the development of the SLES as described below:

In Phase I, NSIR sponsored an initial proof of concept activity to evaluate feasibility and operational considerations, explore options, and conduct an analysis of potential alternatives and implementation concerns.

In 2005, NSIR sponsored the E-Safe Pilot, which provided a limited secure electronic repository for SGI documents. The E-Safe Pilot used a version of the NRC's FileNet platform for unclassified electronic document management and was installed in a secured room which could be accessed

by authorized NSIR users. The E-Safe Pilot successfully demonstrated potential benefits, but was limited as a standalone system in a secured environment.

In 2006, NSIR sponsored an SGI LAN proof of concept for wireless connections by authorized users from their workstations to the SGI document repository. Keyboard Video Mouse (KVM) switch and Smart Card technologies used in the proof of concept provided secure access with user authentication controls.

In 2006, NSIR sponsored the development of the SLES investment Business Case based on the earlier pilot and proof of concept experience, lessons learned, alternatives analysis and cost benefit justification. The NRC senior management approved the SLES Business Case in December 2006 for phased development of a full production SLES capability. This marked the completion of phase I.

In 2007, NSIR moved forward with the development of the SLES 60 user pilot which included SGI LAN pilot and E-Safe implementation. In August of 2007, the Authorization to Operate (ATO) for the SGI LAN pilot was granted as a General Support System (GSS). In June of 2008, the ATO for the E-Safe application was granted. The SLES system sensitivity has been categorized as high security baseline (confidentiality – high, integrity – moderate, and availability - moderate) and is currently being maintained in operation for NSIR pilot users in accordance to the terms of the Security Plan and the ATO approval. The E-Safe application is using Documentum, a Commercial Of-The-Shelf software package, to provide full document and records management capabilities and to meet the NRC security requirements for electronic SGI documents. During FY2008 - FY2011, NSIR will implement SLES into the NRC Production Operating Environment (POE) at headquarters and the regional offices via an implementation contract which shall increase the number of users from approximately 100 to 600 users. NSIR will then expand use of the SLES by providing access to authorized Federal, State and Local Government Agencies and Licensees, increasing the number of users from approximately 600 to 1,000.

## **2 System Overview**

The SGI LAN operates as a General Support System (GSS). This network capability provides encrypted and secure communications from thin client devices to the host servers. KVM switches are used to isolate the SLES network from the NRC network at the user's workstation along with strong user authentication controls through Smart Card, NRC Managed Private Key Infrastructure (MPKI), and hardened network operating systems. In the future, remote users on encrypted channels may access a secure web service which provides secure Internet portal access. Secure access from regional offices will be supported by encrypted tunnel controls. Secure access for external users will be supported by a highly secure out-facing segment of the LAN DeMilitarized Zone (DMZ).

The E-Safe application operates as a Major Application and is connected to the SGI LAN. E-Safe provides fully featured electronic document and record management functionality to users with secure access authorization. Management of user and group accounts are provided as an Administration services capability.

NSIR is implementing the SLES project in three development phases:

- Phase I completed the development of the E-Safe pilot, the SGI LAN proof of concept, and the development of the SLES Business Case.
- Phase II\* includes the implementation and rollout of the SLES solution to authorized NRC Headquarters and regional users; also evaluates external access policies and procedures for access by Federal, State and local agencies, and Licensees.
- Phase III\* includes the implementation and rollout of the SLES solution to authorized external Federal, State, and local agencies and Licensee representatives. The candidate solution will be subject to the successful evaluation and coordination with the Office of Information Services (OIS), the Computer Security Office (CSO) and other stakeholders.

\* This O&M contract is to provide support during Phases II and III of the SLES project.

### 3 Objective

The objectives of this SLES operation and maintenance service contract are to:

- Transition SLES from current contractors to operate under a new Support Agreement
- Provide system and security administration services for the SLES in Operation as it continues to be developed and expanded from the current limited number of users at the NRC HQ to full deployment to users at the regional offices as well as other authorized Federal, State and Local Government Agencies and Licensees
- Ensure that all system modifications, particularly addition of Wireless Access Points (WAPs) maintains required computer security controls
- Ensure that expansion from the current floors/building to additional floors and NRC buildings maintains required computer security controls
- Maintain an operational status for all SLES system components
- Provide Help Desk support services to the SLES users
- Manage system configuration and maintain/update system documentation
- Provide operation and maintenance support for the secure SGI records repository in compliance with National Archive and Records Administration requirements
- Provide operation and maintenance support for management (add, store, search, retrieve, collaborate, and disposition) of SGI documents in a centralized electronic document management system using Documentum software
- Provide Disaster Recovery services for the SLES system.

To accomplish the above objectives, the primary requirements for this procurement shall be:

1. Acquisition of expert-level system administration, and operations support services to operate and maintain the SLES using the state-of-art technology in a cost effective way.
2. Acquisition of expert-level security administration and controls to comply with the SLES security requirements and to protect the NRC from unauthorized access to the Agency's Safeguards information.

### 4 Scope of Work

The scope of work for this contract includes all required and necessary tasks to maintain the SLES

system and to ensure its operability for its users. It consists of, but not limited to, daily system and security administrative activities, tasks and activities for maintaining the SLES equipment Hardware (HW) and Software (SW) and operational users support.

The contractors shall provide, at a minimum, the described services and perform the tasks listed in this statement of work. During the life of this contract, NRC continues to further develop and gradually deploy SLES to users in the Headquarters and regions; and eventually to all other authorized users in Federal, State and local agencies, and Licensees.

The contractor shall be providing O&M support services for the SLES deployment to approximately 1,000 users by the end of the contract period.

## 5 General Requirements

1. The contractor shall maintain continuous availability of all key personnel for performing required tasks and to provide the services described in this Statement of Work (SOW). The contractor shall ensure that both key and backup personnel are committed in providing operations and maintenance support services between 7:00 A.M. and 5:00 P.M., Eastern Time, Monday through Friday (with the exception of Federal holidays). All service requests (telephone call, email, or other means of communication) must be responded to by the contractor within a 60 minute time-frame from the time that the service request was received.

In case of emergencies or for reasons related to system repair/maintenance, the contractor may be called or required to work outside of the regular hours of operations as mentioned above.

2. Under this Operations and Maintenance contract, the following rules of behavior must be adhered to by the contractor's personnel at all times during the life of the contract. The contractor shall also ensure that the system is in compliance with Management Directive 12.5. Administrators shall:
  - Report all security incidents and potential threats and vulnerabilities involving the SLES immediately to the NRC system designated Information System Security Officer (ISSO)
  - Protect system from access by unauthorized users
  - Ensure that system media and system output are properly marked, controlled, and stored per NRC MD 12.5 and 12.6
  - All handling of SGI must conform to NRC policy, standards, and guidance, in particular MD 12.5, 12.6 and MD 12.7.

Administrators shall not attempt to:

- Introduce malicious code into the SLES or physically damage the network
- Bypass, strain, or test security mechanisms; any ongoing or regular bypass of security mechanisms will be approved by the Designated Approving Authority
- Introduce or use unauthorized software, firmware, or hardware on the SLES

- Assume the roles and privileges of others and attempt to gain access to information for which they have no authorization.
3. The contractor staff shall adhere to and implement all documented required security measures in their activities as set forth by the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST), and the NRC throughout the life of the contract.
    - The contractor shall address and comply with all NIST 800-53 requirements consistent with high baseline security controls and additional controls as deemed necessary by the sensitivity of information being processed and the nature of the system. This includes maintaining and correcting security controls as requirements.
    - The contractor shall meet the Continuous Monitoring requirements identified in NIST Special Publication 800-37.
    - The contractor shall maintain the SLES system security plan and develop any other type of system security and operational documentation as requested by the NRC system owner or system owner designee.
  4. The contractor shall have trained staff in Information Technology (IT) security aspects and controls for the operating systems, devices, and applications used in this system assigned to this contract
  5. The contractor shall adhere to and apply the NRC Project Management Methodology (PMM) throughout the life of the contract. The PMM provides important system development guidance for all NRC IT programs across the life cycle from initial concept to retirement and defines key milestones, activities and deliverables. See the PMM White Paper attachment 1 to this SOW for an overview of the PMM.
  6. The contractor shall coordinate their activities with other NRC internal offices, such as, OIS, Computer Security Office (CSO), and the Office of Administration (ADM). The contractor shall work with various NSIR staff and other contractors that may be active on SLES.
  7. The contractor shall perform work under this agreement in such a manner to assure the SLES system availability at 99% quarterly throughout the life of the contract. However, the contractor is expected to report on the system availability on a monthly basis as part of the status reporting requirement under section 7 of this SOW.

The SLES system availability shall be defined as:

**System operable time divided by (System operable time + system inoperable time)**

For the above calculation, the operable and inoperable time of the system is measured between 7:00 A.M. and 5:00 P.M., Local Time, Monday through Friday (with the exception of Federal holidays). SLES shall not be considered inoperable when the cause of failure is outside the scope of this contract (e.g. extended power failure, agency wide down time to unforeseen events, etc.)

**NRC-07-09-136 - Enclosure 1 – SOW**

Failure to achieve this standard over a time period of 3 months will be subject to the following deductions:

<b>Threshold for the system inoperability</b>	<b>Quarterly applicable deduction</b>
80% - 89.99%	1% of the total monthly billable amount by the contractor for services rendered to maintain the System, task 6.4 in this SOW.
75% - 79.99%	3% of the total monthly billable amount by the contractor for services rendered to maintain the System, task 6.4 in this SOW.
74.9% or below	10% of the total monthly billable amount by the contractor for services rendered to maintain the System, task 6.4 in this SOW.

## 6 Tasks

### 6.1 Transition SLES to Operate Under a New Support Agreement

The tasks described below are required to transition SLES from the current NRC O&M contract to this contract.

#### 6.1.1 Kick-off meeting

The contractor shall attend a kick-off meeting within 5 working days after award to introduce staff and to present their general approach in meeting the requirements delineated in this Statement of Work (SOW). As an outcome of this meeting, the contractor shall develop and submit to the NRC Project Manager a document entitled "Project Coordination and Integration" outlining the contractor's approach, resource allocations and coordination plan and adherence to the NRC Project Management Methodology to meet the requirements of this project. This document will be revised to reflect the project start date agreed by both parties.

<b>Item</b>	<b>Deliverable</b>	<b>Estimated Delivery Schedule</b>
1	Attend Kick-Off Meeting at NRC HQ	5 working days after award
2	Project Coordination and Integration document	5 working days after project start date

### 6.1.2 *Operating plan*

The contractor shall prepare a comprehensive transition plan for the system Operations and Maintenance from the current O&M contractor. This plan should include the overall approach for the transition including shadowing, reviewing the procedures and conducting a gap analysis.

The contractor shall prepare and submit in writing to the NRC project officer a detailed operating plan for providing the O&M support activities as outlined in this SOW. The operating plan must include contractor's compliance with the general requirements as stated in section 5 of the SOW and delineate all tasks and deliverables, as well as the required staff and the operating procedures to execute the tasks or provide the required services under this task order.

Item	Deliverable	Estimated Delivery Schedule
1	Transition Plan	1 week after project start date
2	Operations and Maintenance Operating Plan	2 weeks after project start date

## 6.2 System Administration

Monitoring the performance of all SLES back-end servers and other equipment, systems programming and configuration management, database administration, security hardening, building of new servers, hardware/software configuration, system backup and restore, system review and making recommendations for performance enhancement are included under this task.

### 6.2.1 *System Performance Monitoring*

The contractor shall continuously monitor the performance of all SLES system hardware and software to identify and resolve problems that may arise on a daily basis. This includes monitoring and testing of the servers and other equipment as the systems continues to be developed and expanded into the POE. The contractor shall be responsible for monitoring and testing of the Wireless Access Points (WAPS) for bleed outside of the facilities approved for wireless SGI processing. Bleed should not be more than 10-15 feet outside the approved buildings. The system administrator shall review all application specific logs associated with the servers (i.e. server logs, database logs). The contractor shall notify the NRC project officer of any problems identified and obtain approval from the NRC project officer before taking actions for resolving them. All incidents, issues or concerns must be recorded by the contractor in the "Maintenance and Activity Log".

The system administrator shall monitor Central Processing Unit, memory and disk performance of all system servers as it expands from the current stage of development to deployment at the regional offices and other authorized Federal, State and Local Government Agencies and Licensees.

**NRC-07-09-136 - Enclosure 1 – SOW**

The administrator shall look for any unusual activity that may represent potential threats or issues with system performance.

The contractor is responsible for maintaining a proactive security stance by accurately documenting routine and non-routine actions occurring on all SLES servers. The Maintenance and Activity Log shall be kept updated for all SLES system servers. All issues identified as a result of these activities will be escalated following the procedures outlined in the system Operations Manual.

The system administrator shall also document all system abnormality occurrences that cannot be accounted for in the audit logs. The information recorded will include the name of the server, the name of the administrator, the date of the occurrence, the details of the abnormality, any actions taken to remedy the situation, whether or not further action is required.

Item	Deliverable	Delivery Schedule
1	Updated Maintenance and Activity Log	As needed
2	Test results/reports	As needed
3	Issue resolution documentation/report	As needed

**6.2.2 System Backup**

This task consists of producing daily (Monday – Friday) incremental tape backup of all the SLES servers and a full backup once a week. System backups must be retained for a period of at least one month on tapes. Please refer to section 6.4 for the short list of the SLES system servers to be administered under this task.

The contractor shall be responsible for managing the rotation (shipping and receiving) of the backup tapes to a geographically remote location from the NRC Headquarters for storage.

Item	Deliverable	Delivery Schedule
1	Set of SLES server backup tapes for each week shipped to be stored in a geographically remote location from the NRC Headquarters	Weekly

**6.2.3 System Recovery**

This task ensures that the data is recoverable from the backup tapes.

**NRC-07-09-136 - Enclosure 1 – SOW**

The contractor designated system administrators (may be referred to the system administrator, administrator or contractor hereafter) shall perform verification tests to restore several different files from the tapes to temporary directories on various servers. The verification test may be performed on the SLES test and development environment when available. Temporary files will be deleted after verification is complete.

Verification tests of the backup system must be performed at least once every quarter and should be documented in the Maintenance and Activities log. Procedures for data recovery “verification” test shall be developed and presented by the contractor to the SLES project manager and the Information System Security Officer (ISSO) for approval.

<b>Item</b>	<b>Deliverable</b>	<b>Delivery Schedule</b>
1	System recovery test results	Quarterly

**6.2.4 Client Terminal Image Backup**

The contractor shall maintain a standard user and kiosk terminal images on backup tapes once a week in order to capture and maintain standard configuration of the terminals.

The system administrator shall identify the standard user and kiosk terminal that the images will be made from. Using the Rapport utility, the system administrator shall create (read) an image of the target user desktop terminal for storage and distribution. Device identification numbers along with the users ID and all other device deployment related data are maintained by the SLES the system administrator in the Rapport server.

<b>Item</b>	<b>Deliverable</b>	<b>Delivery Schedule</b>
1	Standard terminal image on tapes	Weekly

**6.2.5 Database Administration**

The contractor shall provide database (SQL server) administration functions on the SLES system. This task includes database structural maintenance activities, adding tables and repositories as needed as well as first line database related support to users, troubleshooting user issues, administering user privileges and assistance to users in generating reports. NRC project manager and ISSO approval must be obtained before changes are made to the database.

<b>Item</b>	<b>Deliverable</b>	<b>Delivery Schedule</b>
1	Ad-hoc database activity report	As needed
2	Updated configuration management document	As needed

6.2.6 *Portal Administration*

The contractor shall maintain an activity log for the portal. The administrator shall review the audit logs located in the Audit Manager of the Administration console weekly and initial the audit log each week indicating that the logs have been reviewed. The administrator will look for any unusual activity, in particular denied logins, review the issues with the system administrator and escalate as necessary.

Item	Deliverable	Delivery Schedule
1	Ad-hoc portal activity report	As needed

6.2.7 *(Optional) Records/Documents (Documentum) Administration*

The contractor shall provide records management and administrative services related to the use of Documentum. The contractor shall work closely with the NRC's project manager to determine and implement the appropriate changes and enhancements to the E-Safe application. The contractor shall also maintain proper set-up and disposition of retention schedules for the E-Safe records in accordance with the NRC's NARA-approved schedules, and NRC Records Management policies.

Item	Deliverable	Delivery Schedule
1	User Requirements and Suggested Enhancements Report	As needed

6.3 *User Support*

6.3.1 *Users Registration and Access Authorization Management*

The contractor designated security administrator shall administer user registration (addition and removal of users) based on established procedures outlined in the SLES Operations Manual. The contractor must also maintain an active SLES user list. This activity includes set up and removal of the SLES user desktop equipment. In conformance with NIST standards, SP 800-53, separation of duties through system access authorization must be assured between the system administrator and the system security administrator who is in charge of access card issuances/cancellations and the system access control administration.

6.3.2 *Help Desk and User Desktop Support*

The contractor shall provide help desk services during the normal business hours of Monday through Friday, 7 a.m. to 5 p.m. through the NRC established phone number and email with dedicated on site staff. The contractor may be asked to support users at anytime after the business hours as requested by the project officer and in case of emergency situations.

**NRC-07-09-136 - Enclosure 1 – SOW-**

The help desk staff shall be responsive to all SLES user requested assistance or reported problems related to the use of the network system. The user requests to the helpdesk are categorized in following table with the corresponding required actions.

Category	Request	Action
High	<ol style="list-style-type: none"> <li>1. Service interruption</li> <li>2. Loss of data</li> <li>3. Security related items</li> </ol>	Shall be reported to NRC project manager immediately
Medium	<ol style="list-style-type: none"> <li>1. Design modification request to include records management, and portal</li> <li>2. User registration/removal</li> <li>3. Equipment deployment</li> </ol>	Shall be reported to NRC project manager before any action taken
Low	<ol style="list-style-type: none"> <li>1. Services</li> <li>2. System access and use</li> <li>3. Equipment related issues</li> </ol>	Action shall be taken to respond to the user request

The service requests may be related to users' registration, smart-card issuance or other concerns surfaced during the audits of the security and system logs. The help desk log shall be a source of information about the actual performance of the system. It must reflect not only the issues reported by the users but also the solutions and the type of actions taken.

The help desk staff shall manage:

- Interface with users and respond to or coordinate actions in response to users request for assistance
- Interface with ISSO, NRC Project Officers, System Administrator and other contractor resources on all operation issues
- Coordinate activities with other NRC offices as needed as instructed by the NRC project manager.

The deliverables include:

Item	Deliverable	Estimated Delivery Schedule
1	Help Desk Log	Shall be maintained on a daily basis
2	Help Desk report and trends	Once a month

Item	Deliverable	Estimated Delivery Schedule
3	User services and suggested enhancements	Once a month
4	Definition of system boundaries and service commitments and escalation paths	4 weeks after project start date
5	Description of in-scope and out-of-scope services for user support	5 weeks after project start date

**6.3.3 (Optional) Record / Document Management and User Desktop Support**

The help desk staff shall provide Records/Document Management support for users using EMC's Documentum product. The contractor shall assist and train users with general use of the applications and troubleshoot specific reported issues related to records/document management. The contractor shall support users with up-loading, down-loading, retrieving documents, and setting up workflows.

The help desk staff shall interface and coordinate activities with NSIR E-Safe processing center in the following areas:

- Process all non-duplicate SGI records submitted for processing into E-Safe
- Provide priority E-Safe support during an Incident Response while the agency is in a Monitoring or Activation mode

**6.3.4 Kiosks Administration and support**

SLES Kiosks, which are accessible by all system authorized users have similar equipment to those at individual user's desktop with certain Input/Output peripherals such as CD and DVD and floppy drives and high speed printer.

The contractor shall maintain all Kiosks (HQ and Regional) operable and respond to all Kiosks related reported problems or service requests by the users in the same way as other service request described above. A record of each service request or reported problem or incident related to Kiosk equipment must be kept in the Maintenance and Activity Log by the contractor.

**6.4 System Maintenance**

The contractor shall maintain all SLES hardware and software on a regular basis in order to ensure continual and reliable system operation. The term "maintain" includes all activities associated with diagnostics, repair or replacement, modification or update and enhancement deemed necessary on the system hardware and software.

The contractor is required to upgrade/refresh system hardware and software to ensure appropriate maintainability and IT security controls. Hardware and software should not be allowed to become unsupported or insecure.

In the event that equipment manufacturer or vendor assistance or services may be required, the contractor must first receive approval from the NRC project manager for the intervention/service. Procurement of vendor services and all replacement parts or equipments are the responsibility of NRC. However, the contractor is expected to provide the exact technical specifications and all other necessary information for procurement of the needed parts and/or services and keeping track of the service coverage warranties and service contract already in place or to be procured for all SLES hardware and Software.

The following is the current list of the SLES primary servers that will need to be maintained in operation:

**Primary Domain Controllers/Certificate Authority**

Dell Power Edge 2850/ Windows 2003, SP1/ Luna PCM Client

**Backup Domain Controllers/Certificate Authority**

Dell Power Edge 2850/ Windows 2003, SP1/ Meta Frame Access Suite License

**File Server**

Dell Power Edge 2850/ Windows 2003, SP1

**MS Exchange server**

Dell Power Edge 2850/ Windows 2003, SP1/MS Exchange 2003

**SQL Server**

Dell Power Edge 2850/ Windows 2003, SP1/ SQL 2005

**Application Server**

Dell Power Edge 2850/ Windows 2003, SP1/ SQL 2005/Activeidentity 4/ Safenet 2.1

**Citrix Server**

Dell Power Edge 2850/ Windows 2003, SP1/ Citrix 4.1/ Management console

**Citrix Server**

Dell Power Edge 2850/ Windows 2003, SP1/ Citrix 4.1/ Management console

**E-Safe SQL Server**

Dell Power Edge 2850/ Windows 2003, SP1/ SQL 2005

**E-Safe Application Server**

Dell Power Edge 2850/ Windows 2003, SP1/ SQL 2005/Documentum

**Administrative portal**

Dell Power Edge 2850/ Windows 2003, SP1/ BEA 6.0

**Automation portal**

Dell Power Edge 2850/ Windows 2003, SP1/ MetaFrame Presentation

**Collaboration portal**

Dell Power Edge 2850/ Windows 2003, SP1/ BEA 6.0

In addition to the above primary servers list, the contractor shall maintain other equipment such as the data storage devices, infrastructure equipment (Cisco 3560 switches, Cisco Wireless LAN Controllers and Wireless Access Points) and the users' desktop and kiosk equipment.

The SLES user desktop equipment consists of a thin client terminal, and a (KVM) switch. SLES Kiosks which are accessible by all system authorized users have similar equipment to those deployed at the user's desktop with certain I/O peripherals such as CD and DVD and floppy drives and high speed printer.

The contractor shall maintain all SLES main server room equipment, floor equipment, and desktop equipment deployed to the users. The contractor shall also maintain all other system related equipment to include the future disaster recovery system as the SLES continues to be developed and deployed into the production environment.

In the event that equipment manufacturer or vendor assistance or services may be required, the contractor must first receive approval from the NRC Project Officer for the intervention/service. Procurement of vendor services and all replacement parts or equipment are the responsibility of NRC. However, the contractor is expected to provide the exact technical specifications and all other necessary information for procurement of the needed parts and/or services and keeping track of the service coverage warranties and service contract already in place or to be procured for all SLES hardware and Software.

System maintenance also includes all required activities in response to the Plan of Action and Milestones (POA&M) which are required to be completed in order to maintain the ATO for the SGI LAN and the E-Safe. The contractor shall evaluate the required actions and present a detailed execution plan for each of the actions to the NRC project manager for approval before taking the actions. Following is the list of scheduled maintenance activities which shall be part of the contractor responsibility and duties under this contract:

#### *6.4.1 Daily Activities*

The system administrator shall review all application specific logs associated with the server (i.e. IIS logs, database logs, etc.). The system administrator is considered key personnel with back up to assure duty coverage at all times.

The system administrator shall review and archive all applications security and system logs associated with the operating system. The system administrator checks for errors, warnings or other events and evaluate if the issue needs to be escalated. Additionally, the administrator shall inspect the logs for potential issues including access attempts (invalid, or valid, after-hours access) and unusual activity. Any significant findings are reported to the SLES designated NRC ISSO and the NRC Project Officer for evaluation and if necessary escalated according to the procedures outlined in the SLES Operations Manual.

In the case when logs were found to be disabled or inoperable on the system, the system must be shut down or interrupt services according to the procedures outlined in the SLES Operations Manual document. The Project Officer and the designated SLES ISSO shall be notified by the contractor before appropriate actions are taken to remedy the situation. When audit logs are returned to normal state, the system administrator may restart or resume services.

The system administrator shall review security sites for vulnerabilities: [www.ciac.org](http://www.ciac.org), [www.cert.mil](http://www.cert.mil), and all appropriate vendor sites. The appropriate vendor sites include all sites for both the operating system and applications that are running on the server(s). These may include [www.microsoft.com](http://www.microsoft.com), [www.BEA.com](http://www.BEA.com) and others.

## **NRC-07-09-136 - Enclosure 1 – SOW**

The system administrator shall evaluate and apply system or application patches as appropriate. Only after NRC approval following the change control procedures in the Configuration Management Plan (CMP), the patch may be installed on the production system.

The system administrator shall monitor RAID integrity and drive availability. Any hard drives that fail will be replaced. Replacement of failed devices must follow Configuration Management procedures outlined in the system Configuration Management Plan.

The system administrator shall verify that system backups have occurred as scheduled. The administrator shall notify the NRC project manager if backups have not occurred and proceed by either running new backups immediately or troubleshooting the issue and running the backups as soon as the issue is resolved.

The system administrator shall change application passwords when any privileged users leave with NRC project manager approval.

### **6.4.2 Weekly Activities**

The system administrator shall update anti-virus definitions whenever new profiles become available. The contractor assures that system backup tapes and other media not being used are stored outside of the server room and rotated on a regular basis. Specific procedures to be followed by the contractor for the handling, storage and the rotation of the backup tapes and media are outlined in the Operation Manual.

The system administrator shall monitor servers' memory storage/used disk space, and delete temp files as necessary. The system administrator should notify the NRC project manager if network resources are being diminished in an unusually rapid fashion or if resources are running low on any device.

The system administrator shall reboot servers (if necessary) and ensure system comes back online and operates normally.

The system administrator shall check management workstation access logs for activities and verify that the usage is not unusual.

### **6.4.3 Monthly Activities**

The contractor shall manage the privileged group accounts access.

The administrator shall monitor activity on user accounts and disable those user accounts that have been inactive for at least 30 days.

The system administrator shall perform a network system scan using NRC CSO scanners and analyzers, DISA Gold Standard to check for network vulnerabilities on the production servers. Any vulnerability found during a scan will be reviewed and acted upon as necessary and in the appropriate time frame according to NRC policy, and the SLES policies on Configuration Management.

### 6.5 Server Shutdown and Restart

The contractor shall be responsible for performing system shutdown and restart. System shutdowns may be required as a planned or unplanned event. Planned servers maintenance shutdowns and other orders may be performed providing that they are pre-approved by the NRC project manager and the NRC ISSO and at least a 24 hours notice is given to the system owner or the designee, the users and other stakeholders. Unplanned shutdown events could be the result of server failure or administration events such as virus infection, audit log failure, loss of power, or security incident investigation. In the event of a power outage, the SLES will rely on an Uninterruptible Power Supply to provide one hour of backup power. This will allow enough time for a graceful shutdown of the servers to prevent loss of information. In the case of either planned or unplanned events, daily maintenance logs must be annotated with the cause and purpose of the event. The NRC project manager and NRC ISSO must be notified in all cases of unplanned shutdown events and it will be the administrator that can authorize restart of one or more system servers.

### 6.6 Disaster Recovery

The contractor shall be responsible for taking the following actions in case of a partial or total interruption of the SLES system operation as a result of system equipment failure due to an unforeseen event.

The system administrator determines the causes and the extent of the damage to the SLES system and submits a remediation plan of action to the NRC project manager for approval.

The system administrator prepares a list of accredited hardware and software to NRC project manager for procurement. Once HW/SW is replaced or (re-)installed, the system administrator must perform all necessary functional tests to ensure that the system is functioning properly.

The system administrator the ISSO and NRC project manager determine what (if any) content on the SLES must be restored from the backup device/tape. Once the data is restored the administrator must perform necessary test to ensure data integrity and total system restoration. The restored content is made available to the SLES users.

All backup and recovery efforts will be documented in the maintenance and activity log.

### 6.7 Configuration Management

The configuration management and change control processes are documented in the SLES configuration management plan. The contractor must follow the policies and procedures outlined in this plan to record any changes in the SLES equipment baseline configuration including operating system and all applications including E-Safe Documentum software. The ISSO is responsible for the security posture of the system. Any changes to the system security posture must be approved by the ISSO. The contractor should not make changes to the system's security posture without the appropriate involvement and approval of the Change Control Board which includes NRC project manager, ISSO, and Senior Information Technology Security Officer.

The contractor shall update the SLES Configuration Management document to reflect all approved configuration changes in the SLES servers, networking equipment, controllers and users' desktop and kiosk equipment.

**6.8 System Documentation Reference and Update**

- The following is a short list of important reference documents that must be reviewed and updated by the contractor periodically. Risk Assessment \*
- Configuration Management Plan
- System Security Plan\*
- Operations Manual\*
- User's Guide
- User's Desktop Reference
- Administrator's Guide
- \* Safeguards Information.

The contractor shall make the necessary changes or updates to these and other existing system documentations at the request of the Project Officer. The changes or updates to these documents and other may be required as a result of system configuration changes or actions taken in response to the SLES (SGI LAN and E-Safe) POA&M's to maintain the system ATO.

Every time a change or update is to be made in an existing system document, the following steps should be followed through by the contractor:

- Necessary changes are made in draft form
- The draft document is submitted to NRC project manager for concurrence
- NRC approved changes are added to the appropriate document

Item	Deliverable	Delivery Schedule
1	Updated system documentations	As needed

**6.9 Transition SLES Operations and Maintenance to OIS**

The tasks described below are required to transition SLES infrastructure O&M to OIS.

**6.9.1 Transition meeting(s)**

At the request of SLES project officer, the contractor shall attend meetings with OIS to present their general approach and work out a detailed transition plan for the SLES infrastructure O&M to OIS.

Item	Deliverable	Delivery Schedule
------	-------------	-------------------

Item	Deliverable	Delivery Schedule
1	Contractor presentation of their approach for transition to OIS	Within two weeks from date of the request by the project officer to start the task

6.9.2 Update the Operating plan

The contractor shall prepare a comprehensive transition plan for the system infrastructure O&M to OIS. This plan should include the overall approach for the transition including shadowing, reviewing the procedures and conducting map and gap analysis.

The contractor shall also review and update as needed the operating plan for providing the O&M.

Item	Deliverable	Delivery Schedule
1	Infrastructure transition plan to OIS	4 weeks from date of the request by the Project Officer to start the task
2	Updated O&M Operating Plan	4 weeks from date of the request by the Project Officer to start the task
3	Transition SLES infrastructure to OIS	6 weeks from date of the request by the Project Officer to start the task

7 Status Meetings and Progress Reporting

- Meetings

The contractor shall schedule, prepare and conduct bi-weekly status meetings with the NRC SLES project management team during which status and progress made in implementing the tasks under contract are presented and discussed. Contractor shall produce minutes of each meeting and shall submit them within three days after each meeting to the Project Officer for concurrence.

At the request of the NRC project officer, the contractor may be requested to attend the projects team meetings, system review and other technical meetings pertinent to the SLES O&M. At a minimum, there will be one system review meeting conducted per quarter throughout the life of the contract that must be attended by the contractor.

The contractor may be requested by the Project Officer to document/produce minutes of these meetings.

Item	Deliverable	Delivery Schedule
1	Meeting minutes and presentation	Bi-weekly
2	System review report/minutes	Quarterly

- **Monthly Status Report**

The contractor shall provide a monthly status report to the NRC project officer and the contracting officer by the 10th day of each month.

The monthly project status report must include at the minimum the following information:

- Highlights of important activities/events which occurred during the reporting period.
- Staffing plan and changes
- Current tasks and deliverable status. This should include the cumulative and current hours of each labor category spent on each task.
- Earned Value calculations
- Projected activity plan for the next reporting period.
- Up-to-date financial status to include prior, current and anticipated expenditures.

Additionally the contractor is required to produce a one page dashboard view of the SLES system status for NSIR management on a monthly basis. The contractor shall also develop a quarterly newsletter to communicate the status of system such as development, expansion and migration efforts. The contractor shall report on document count, user adoption rate, files created per month, files uploaded and retrieved per month, help desk calls and other information as requested by the project officer.

Item	Deliverable	Delivery Schedule
1	O&M Status report	Monthly
2	Dashboard	Monthly
3	Project Newsletter	Quarterly

## 8 Procurement Responsibilities

The NRC will be responsible for procurement of all necessary equipment (hardware and/or software) for the operation, maintenance and testing of the SLES system.

## 9 Contractor Personnel Skill Set Requirements

The contractor staff shall possess and demonstrate experience and knowledge to meet the following skill set requirements:

**NRC-07-09-136 - Enclosure 1 – SOW**

- Extensive experience in project management (PMP certification is desired)
- Extensive experience and knowledge of network design, security, wireless communications and wi-fi technologies and devices
- Extensive experience in maintaining and enhancing Enterprise Content Management systems, specifically Documentum based applications to include implementing new modules of Documentum (for example: Business Process Manager and Information Rights Manager).
- Experience in managing and disposing of electronic records to National Archive Records Administration (NARA)
- Experience in maintaining secure, FISMA compliant networks and applications to include knowledge of maintaining certified and accredited systems
- Experience in managing and running helpdesk services for geographically dispersed users
- Extensive experience in system analysis, development, and deployment techniques for information technologies and secure network distributed systems
- Experience in maintaining a secure Web Portal system
- Experience with developing administration and operations support procedures for secure wireless networks and document management applications
- Experience with training end-users

The contractor shall demonstrate knowledge and experience with applying and compliance with federal standards for security specifications including:

- a) FIPS 140-2, NIST Encryption Standards
- b) FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- c) FIPS 200 Minimum Security Controls for Federal Information Systems
- d) NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002
- e) NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
- f) NIST SP 800-60, Volume II: Guide for Mapping Types of Information and Information Systems to Security Categories
- g) NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems
- h) NIST SP 800-26 Security Self-Assessment Guide for Information Technology Systems
- i) NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal

Information Systems

- j) NIST SP 800-47 Security Guide for Interconnecting Information Technology Systems
- k) NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- l) NIST SP 800-64 Security Considerations in the Information System Development Life Cycle
- m) DOD 5015.2 and NARA requirements for the electronic recordkeeping systems
- n) Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources
- o) DOD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)
- p) Additional issuances from the Committee on National Security Systems relevant to classified systems
- q) Federal Information Security Management Act 2002
- r) NRC Management Directive 12.5, 12.6, etc. (to be furnished upon contract award)

(<http://www.nrc.gov/reading-rm/doc-collections/management-directives/volumes/vol-12.html>)

In addition, the contractor personnel skill sets shall demonstrate strong communications and interpersonal skills. The contractor manager and designated staff shall be required to meet with, discuss, and obtain information required to accomplish the tasks described in this statement of work, which will involve regular communications – formal and informal – with senior NRC staff members. The contractor manager and designated staff are required to communicate, coordinate, and collaborate with security experts within the NRC Office of Information Services (OIS) to ensure that the SLES production system follows the NRC security standards and meets the compliance requirements with security regulations.

## 10 Protection of Proprietary Information

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

## 11 System Security and Requirements for Handling SGI

The contractor shall comply with the following security requirements:

- The SLES system must meet all federally mandated and NRC defined security requirements.

**NRC-07-09-136 - Enclosure 1 – SOW**

- All system modifications must comply with NRC security policies and procedures for a high sensitivity system and the requirements for SGI processing as directed by NRC policy, regulations, standards and guidance, including MD 12.5, MD 12.6 and MD 12.7, and 10 CFR 73.21, as well as applicable federal laws.
- All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the system sensitivity level.
- The contractor shall ensure that its employees, in performance of the contract, receive IT security training in their role (e.g. system administrators must receive training in the IT security of the operating system, devices, and applications being used).
- The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any protections either designed or developed by the contractor under this contract or otherwise provided by the government. The System Security Plan and other information system security documentation for the contract are considered Sensitive Unclassified Information. The contractor agrees to abide by NRC regulations for handling sensitive unclassified information governed by the NRC's Sensitive Unclassified Non-Safeguards Information program and NRC's MD 12.5, "NRC Automated Information Security Program."
- The contractors shall only use NRC provided e-mail accounts to send and receive information considered sensitive or shall use other NRC approved encrypted means.
- Separation of duties for the systems must be enforced by the system through assigned access authorizations.
- The information system shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.
- The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.
- The contractor shall only use licensed software and in-house developed authorized code (including government and contractor developed) on the system and for processing government information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the NRC DAA. The contractor shall provide proof of licensing upon request of the contracting officer, the NRC project manager, the SITSOs, or the DAAs.
- All development and testing of the systems shall be performed on a network separate and isolated from the NRC operational network that is protected at the high sensitivity in conformance with the requirements for SGI processing as directed by NRC policy, standards, and guidance, in particular MD 12.5 and MD 12.7. .
- An independent tester will be required to perform the security test, evaluation, and contingency testing on the system. The contractor shall support OIS in its efforts to certify and accredit the systems under FISMA as High Impact Major Application by assisting with the completion of required security deliverables that include Memorandum of Understandings, Interconnection Security Agreements, Security Categorization, E-Authentication Risk Assessment, Security Risk Assessment, System Security Plan, Contingency Plan, Security Test and Evaluation Plan, Security Test and Evaluation Execution Report, Contingency Scenario Execution Report, Corrective Actions Plan and Certification Letter.

## NRC-07-09-136 - Enclosure 1 – SOW

- The contractor shall support the NRC in its effort to conduct security tests and evaluation, and contingency tests as needed, to ensure system certification and for continuous monitoring activities. The contractor will provide assistance to the NRC and/or security contractor responsible for developing and performing the test. Tests performed and test results/reports, issue resolution documentation, and updated system documentations are deliverables on the contract by the contractor as mentioned in section 6.2 of this document.
- User accounts that have system-level or administrative privileges must have a unique password from all other accounts held by that user, and general user tasks must be performed from a general user account, not from the administrative account.
- The contractor shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).
- All sensitive data being transmitted over a network by the system shall use FIPS 140-2 validated encryption. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.
- All media produced must include appropriate markings to indicate the sensitivity of the information contained on the media and the media must be controlled according to that sensitivity.
- All information must be cleared off of (wiped) any systems not provided to NRC at the end of the contract. Simple deletion is insufficient. If any SGI information is stored on contractor systems, the media must be rendered to the project manager or destroyed by NRC ADM/DFS at the end of the contract.

## 12 Travel

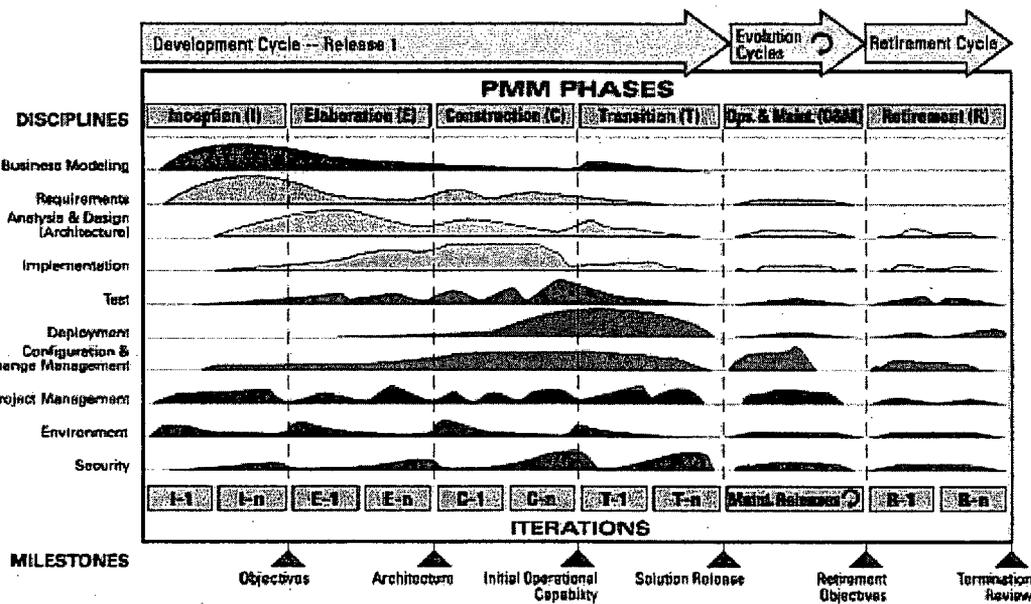
It is estimated that up to ten (10) one-person, two-day trips per year may be required to attend meetings or work with NRC personnel at Region I (King of Prussia, PA), Region II (Atlanta, GA), Region III (Lisle, IL), and Region IV (Arlington, TX). All project related travels including those related to training of users under this contract will be reimbursed in accordance with Federal Travel Regulations. Travel may be required during the course of the contract execution from the NRC Headquarters (Rockville, MD.) to the Regional Offices as required. All travel requests must be submitted to the NRC Project Officer for approval a minimum of 3 days before the requested date of the travel. The contractor shall comply with specific travel requirements defined in the approved SLES Travel Plan, which is a part of the Project Coordination and Integration deliverable.

## PMM Overview

Project Management Methodology (PMM) provides the methods and processes for implementing details for **NRC Management Directive 2.8, "Project Management Methodology"**, and its associated **Handbook, the PMM Manual** (Link is provided below)  
[http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU\\_ADAMS^PBNTAD01&ID=071900874](http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=071900874).

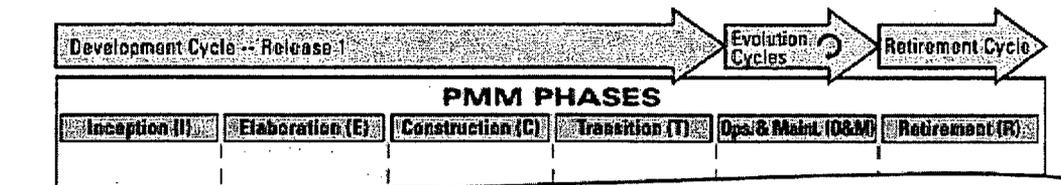
This single Management Directive includes both the policy and a configurable process with guidance, tools, and templates to support the implementation of that process. The PMM initiative is a direct response to concerns raised by agency staff to reduce the burden of IT project management. Further, PMM provides an integrated solution for IT system development.

PMM is organized into a series of phases, each of which is conducted in one or more iterations. During each phase, activities are performed and artifacts produced which align with disciplines, such that each discipline can be viewed as having a work-flow of its own across the life cycle. The humps in the diagram below represent how the emphasis in activities varies over time. For example, in early iterations, you spend more time on requirements, whereas in later iterations you spend more time on implementation.



## Process Cycles

The PMM defines three process cycles — Development Cycle, Maintenance Cycle, and Retirement Cycle. The process cycles represent a way of organizing PMM phases and activities to accomplish specific goals.



## Development Cycle

A development cycle is one pass through the Inception Phase, Elaboration Phase, Construction Phase and Transition Phase; each pass through the four phases produces a generation of the software (or a system release). The system will evolve into its next generation by repeating the same cycle of Inception, Elaboration, Construction and Transition.

## Maintenance Cycle

The subsequent cycles are called evolution cycles. Evolution cycles typically have much shorter Inception and Elaboration phases, since the basic product definition and architecture are determined by prior development cycles. The Maintenance Cycle also has Inception, Elaboration, Construction, and Transition phases, but on a smaller scale than new development. The activities and artifacts build upon existing releases and artifacts supporting those releases. The Operations & Maintenance Phase phase description defines the Maintenance Cycle during Inception through Transition phases as detailed below:

- Inception Phase for Maintenance Projects
- Elaboration Phase for Maintenance Projects
- Construction Phase for Maintenance Projects
- Transition Phase for Maintenance Projects

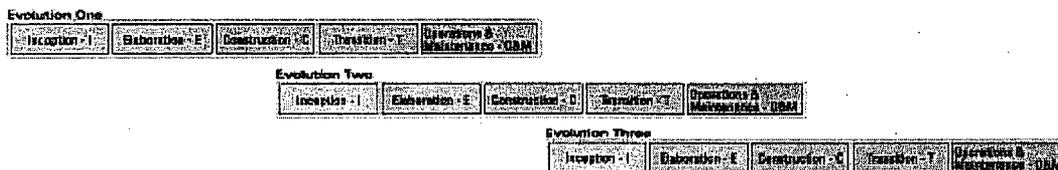
## Retirement Cycle

The Retirement Cycle is a single phase cycle implemented to either eliminate a large part of a system or, as in most cases, close down a system and end the life cycle process. The Retirement Phase description defines this single phase cycle and its activities.

## Process Cycle Planning Considerations

Some projects lend themselves to being managed as multiple evolution cycles (staged functionality, or maintenance cycles) that produce deployed generations of the system. The first development cycle of such projects will spend more time in Inception and Elaboration to address the overall System vision and architecture. Subsequent evolution cycles will have shorter Inception and Elaboration cycles. Many supporting artifacts will be generated in the first development cycle. Following evolution cycles will update these artifacts and flesh out details as needed for that cycle.

For large projects, a pre-planned set of generations may overlap to deploy functionality over time as a series of releases.



In some projects you will want to re-scope and re-justify the effort, hence you will want to spend time in the Inception phase and make updates to the project vision. Other times you may just need to rework the requirements and the architecture for the new release, hence you will put an emphasis on the Elaboration phase. If you have a simple enhancement that adds to existing requirements or use cases, you can quickly step through Inception and Elaboration to update requirements and plans and spend

most of the time in the Construction phase for your new release performing analysis, design, implementation and test.

## **Best Practices**

### **1 - Develop iteratively**

Developing in iterations allows projects to address risks on a priority basis. It allows for a constant measuring of progress, as iterations have a fixed time window and a specific goal to be met. At the end of each iteration, stakeholders are provided a view of how the project is proceeding and can set realistic expectations for the remainder of the project based on the actual progress of working code.

### **2 - Manage requirements**

A key to delivering a system that meets the stakeholders' needs is identifying and then managing the requirements for the system. This includes gathering, documenting, and maintaining of requirements, incorporating changes in a systematic manner, and potentially even tracking and tracing the requirements to the design. Your requirements management process can be very well defined and prescriptive, often involving significant effort and expense but with the benefit of producing accurate and detailed documentation of your decisions; it also can be something as simple as a Vision document for a small system. The PMM can and should be tailored to meet a project's exact needs.

### **3 - Promote an architectural vision**

The PMM uses the term "use component architecture," but the reality is that much architecture isn't component-based. The true best practice is to identify and then prove through prototyping an architecture that is appropriate for the system that you are building.

### **4 - Continuously verify quality**

Testing happens throughout a PMM project as part of iterations instead of a single, large testing effort at the end. Ensuring quality goes beyond testing software to ensure it meets requirements - reviews of requirements, design, and user interface mockups or demos with stakeholders are also part of continuous quality verification. Testing for and catching defects early is much more efficient than a comprehensive approach to testing at the end.

### **5 - Manage change**

Change is a given in software development. Change must be expected and handled appropriately for a project to run smoothly and to take advantage of changes that may improve the business. A wide range of artifacts - documents, models, plans, tests, code, and so on - will potentially be affected by any changes. The project must assess and adjust the plans to accommodate changes.

### **6 - Manage risk**

Effective project teams strive to identify and then manage the risks that they face, either mitigating them completely or reducing their potential impact as appropriate.

### **7 - Develop collaboratively**

Systems are built by teams of people, and if these people don't work together effectively, the overall project risks failure. Security and EA staff must be included early in the process. Encourage active

stakeholder participation, which promotes the concept that project stakeholders should provide information and make decisions in a timely manner and be involved with the development effort itself.

## Benefits

By being scaleable to projects of different sizes and complexities, PMM will help project teams understand what is required of them and what activities and artifacts provide value to their efforts.

- Risks are handled early.
- Focuses on delivering value to the customer.
- Evolves and validates requirements through iterative development.
- Facilitates testing early and testing often.
- Accommodates changes throughout the project.
- Minimizes rework.
- Fosters early verification of the system architecture.
- Encourages team work among contributors.
- Provides consistency through a common vocabulary.
- Continuing focus on quality throughout the project, not just at the end

## Key Objectives

- Eliminate confusion and redundancy with a simple, easy-to-understand process.
- Reduce the burden associated with IT development activities.
- Support flexibility for differing size and complexity of projects.
- Allow individual business offices to build upon minimum requirements.
- Enable more accurate project prediction for planning and budgetary purposes.
- Promote better horizontal and vertical integration across offices and divisions within the agency.
- Ease compliance with applicable regulations, guidance, and directives.
- Increase consistency of IT management practices.

## Additional Benefits

- Useable and useful
- Minimizes the amount to be done for any given project
- Not "One size fits all"
- Repeatable and predictable
- Flexible and suitable for many types of projects
- No need to reinvent the wheel on every project, resulting in an overall better use of time
- Up-front planning saves time and rework later
- Activity-driven *versus* document-driven
- Reduces the burden of previous methodologies
- Improved customer satisfaction through ongoing customer involvement
- Focused on the solution, the business problem to be solved
- Increased communication across groups, leads to better working relationships
- Doing the right thing, at the right time, in the right way

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

**A.1 CONSIDERATION AND OBLIGATION**

(a) The total estimated amount of this order (ceiling) for the products/services ordered, delivered, and accepted under this order is \$702,794.80.

(b) The amount presently obligated with respect to this order is \$300,000.00. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this order. The obligated amount shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this order. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

**A.2 PROJECT OFFICER AUTHORITY (NOVEMBER 2006)**

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

**Primary NRC Project Manager**

Name: **Behrouz Golchane**  
Address: **U.S. Nuclear Regulatory Commission  
11545 Rockville Pike  
Mail Stop: T4-A57  
Rockville, MD 20852**  
Telephone Number: **(301) 415-6196**

**Alternate NRC Project Manager**

Name: **Roya Noory**  
Address: **U.S. Nuclear Regulatory Commission  
11545 Rockville Pike  
Mail Stop: T4-A57  
Rockville, MD 20852**  
Telephone Number: **(301) 415-6868**

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

(1) Technical direction to the contractor which shifts work emphasis between areas of work or tasks, authorizes travel which was unanticipated in the Schedule (i.e., travel not contemplated in

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

the Statement of Work (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

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

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

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

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

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

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

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

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

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

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

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

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

- (1) Monitor the contractor's technical progress, including surveillance and assessment of performance, and recommend to the contracting officer changes in requirements.
- (2) Assist the contractor in the resolution of technical problems encountered during performance.
- (3) Review all costs requested for reimbursement by the contractor and submit to the contracting officer recommendations for approval, disapproval, or suspension of payment for supplies and services required under this contract.
- (4) Assist the contractor in obtaining the badges for the contractor personnel.
- (5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination.
- (6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.
- (7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the contractor as part of closeout procedures, written certification that the contractor has returned to NRC, transferred to the successor contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

**A.3 2052.215-70 KEY PERSONNEL (JAN 1993)**

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

- |                      |   |
|----------------------|---|
| <b>Maher Darwish</b> | <b>Project Manager</b>                              |
| <b>Bruce Jones</b>   | <b>Engineer/Network Administrator</b>               |
| <b>Frank Little</b>  | <b>Network Security Analyst (Help Desk Manager)</b> |
| <b>Bryan Dowdy</b>   | <b>Product Specialist (Documentum)</b>              |

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding **30** work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

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

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

**A.4 2052.215-78 TRAVEL APPROVALS AND REIMBURSEMENT –  
ALTERNATE 1 (OCT 1999)**

(a) Total expenditure for travel may **not** exceed ~~\$15,000.00~~ without the prior written approval of the contracting officer. All Travel **must** be approved in advance by the NRC Project Officer.

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

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

(d) It is the responsibility of the contractor to notify the contracting officer in accordance with the FAR Limitations of Cost clause of this contract when, at any time, the contractor learns that travel expenses will cause the contractor to exceed the travel ceiling amount identified in paragraph (a) of this clause.

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

**A.5 2052.209-73 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST**

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

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

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

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

(c) Work for others.

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

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

(3) When the contractor performs work for the NRC under this contract at any NRC licensee or applicant site, the contractor shall neither solicit nor perform work in the same or similar technical area for that licensee or applicant organization for a period commencing with the award of the task order or beginning of work on the site (if not a task order contract) and ending one year after completion of all work under the associated task order, or last time at the site (if not a task order contract).

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

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

(d) Disclosure after award.

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

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

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

(e) Access to and use of information.

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

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

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

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

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

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

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

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

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

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

**A.6 2052.204-70 SECURITY (MARCH 2004)**

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

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

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

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

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

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

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

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

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

**A.7 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MARCH 2006)**

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

**A.8 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS  
APPROVAL (FEBRUARY 2004)**

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

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

**SECURITY REQUIREMENTS FOR LEVEL I**

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

The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access. Such contractor personnel shall be subject to the NRC contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and will require a favorably adjudicated Limited Background Investigation (LBI).

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

Any questions regarding the individual's eligibility for IT Level I approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E. O. 12968.

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

**SECURITY REQUIREMENTS FOR LEVEL II**

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

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions. Such contractor personnel shall be subject to the NRC contractor personnel requirements of MD 12.3, Part I, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Access National Agency Check with Inquiries (ANACI).

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

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

**CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST**

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

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

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

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

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

**Enclosure 2 - ADDITIONAL TERMS AND CONDITIONS**

**A.10 52.217-9 OPTION TO EXTEND THE TERM OF THE TASK ORDER**

(a) The Government may extend the term of this contract by written notice to the Contractor within 60 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 10 years.

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

**General:** During performance and through final payment of this contract, the contractor is responsible for the accuracy and completeness of data within the Central Contractor Registration (CCR) database and for any liability resulting from the Government's reliance on inaccurate or incomplete CCR data.

The contractor shall prepare vouchers/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

**Form:** Claims shall be submitted on the payee's letterhead, voucher/invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal-- Continuation Sheet."

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

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

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

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

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

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

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

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

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

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

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

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

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

Final vouchers/invoices shall be marked "FINAL VOUCHER" or "FINAL INVOICE".

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

Supersession: These instructions supersede any previous billing instructions.

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

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

**1. Official Agency Billing Office**

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

**2. Voucher Information**

- a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the Payee to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.
- b. Payee's Name and Address. Show the name of the Payee as it appears in the contract and its correct address. If the Payee assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the Central Contractor Registration (CCR) database at <http://www.ccr.gov> and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).
- c. Contract Number. Insert the NRC contract number.
- d. Voucher/Invoice. The appropriate sequential number of the voucher/invoice, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.
- e. Date of Voucher/Invoice. Insert the date the voucher/invoice is prepared.
- f. Billing period. Insert the beginning and ending dates (day, month, and year) of the period during which costs were incurred and for which reimbursement is claimed.
- g. Required Attachments (Supporting Documentation).** Direct Costs. The contractor shall submit as an attachment to its invoice/voucher cover sheet a listing of labor categories, hours billed, fixed hourly rates, total dollars, and cumulative hours billed to date under each labor category authorized under the contract/purchase order for each of the activities to be performed under the contract/purchase order. The contractor shall include incurred costs for: (1) travel, (2) materials, including non-capitalized equipment and supplies, (3) capitalized nonexpendable equipment, (4) materials handling fee, (5) consultants (supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval); and (6) subcontracts (include separate detailed breakdown of all costs paid to approved subcontractors during the billing period) with the required supporting documentation, as well as the cumulative total of each cost, billed to date by activity.

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

**3. Definitions**

- a. Non-capitalized Equipment, Materials, and Supplies. These are equipment other than that described in number (4) below, plus consumable materials, supplies. List by category. List items valued at \$1,000 or more separately. Provide the item number for each piece of equipment valued at \$1,000 or more.
- b. Capitalized Non Expendable Equipment. List each item costing \$50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) the item number for the specific piece of equipment listed in the property schedule of the contract; or (b) the Contracting Officer's approval letter if the equipment is not covered by the property schedule.
- c. Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures.

---

**Sample Voucher Information (Supporting Documentation must be attached)**

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

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

<b>BASE YEAR - (03/06/2009 - 03/05/2010)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		Hour		
Sr. Network Engineer	Engineer/Network Administrator - Key		Hour		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		Hour		
SPI Analyst	Product Specialist (Documentum) - Key		Hour		
<b>SUBTOTAL - LABOR</b> (including OPTIONAL SOW Tasks 6.2.7 & 6.3.3, which are hereby exercised)					<b>\$ 687,794.80</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE	\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - BASE YEAR</b>					<b>\$ 702,794.80</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 1 - (03/06/2010 - 03/05/2011)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		HOUR		
Sr. Network Engineer	Engineer/Network Administrator - Key		HOUR		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		HOUR		
<b>SUBTOTAL - LABOR</b>					<b>\$ 489,908.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE	\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 1</b>					<b>\$ 504,908.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 243,432.00</b>
<b>TOTAL VALUE - OPTION YEAR 1 (Including Optional Tasks)</b>					<b>\$ 748,340.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					

<b>OPTION YEAR 2 - (03/06/2011 - 03/05/2012)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		Hour		
Sr. Network Engineer	Engineer/Network Administrator - Key		Hour		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		Hour		
<b>SUBTOTAL - LABOR</b>					<b>\$ 509,489.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE	\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 2</b>					<b>\$ 524,489.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 253,152.00</b>
<b>TOTAL VALUE - OPTION YEAR 2 (Including Optional Tasks)</b>					<b>\$ 777,641.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 3 - (03/06/2012 - 03/05/2013)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		Hour		
Sr. Network Engineer	Engineer/Network Administrator - Key		Hour		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		Hour		
<b>SUBTOTAL - LABOR</b>					<b>\$ 529,844.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE	\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 3</b>					<b>\$ 544,844.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 263,268.00</b>
<b>TOTAL VALUE - OPTION YEAR 3 (Including Optional Tasks)</b>					<b>\$ 808,112.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 4 - (03/06/2013 - 03/05/2014)</b>					

GSA SCHEDULE 70 LABOR CATEGORY	FUNCTIONAL LABOR CATEGORY	ESTIMATED QUANTITY	UNIT	(Discounted) UNIT PRICE*	TOTAL ESTIMATED COST
Senior PMO Consultant	Project Manager - Key		HOUR		
Sr. Network Engineer	Engineer/Network Administrator - Key		HOUR		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		HOUR		
<b>SUBTOTAL - LABOR</b>					<b>\$ 551,005.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)					1 LOT NTE \$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 4</b>					<b>\$ 566,005.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 273,798.00</b>
<b>TOTAL VALUE - OPTION YEAR 4 (Including Optional Tasks)</b>					<b>\$ 839,803.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 5 - (03/06/2014 - 03/05/2015)</b>					
GSA SCHEDULE 70 LABOR CATEGORY	FUNCTIONAL LABOR CATEGORY	ESTIMATED QUANTITY	UNIT	(Discounted) UNIT PRICE*	TOTAL ESTIMATED COST
Senior PMO Consultant	Project Manager - Key		HOUR		
Sr. Network Engineer	Engineer/Network Administrator - Key		HOUR		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		HOUR		
<b>SUBTOTAL - LABOR</b>					<b>\$ 573,030.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)					1 LOT NTE \$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 5</b>					<b>\$ 588,030.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 284,742.00</b>
<b>TOTAL VALUE - OPTION YEAR 5 (Including Optional Tasks)</b>					<b>\$ 872,772.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 6 - (03/06/2015 - 03/05/2016)</b>					
GSA SCHEDULE 70 LABOR CATEGORY	FUNCTIONAL LABOR CATEGORY	ESTIMATED QUANTITY	UNIT	(Discounted) UNIT PRICE*	TOTAL ESTIMATED COST
Senior PMO Consultant	Project Manager - Key		Hour		

Sr. Network Engineer	Engineer/Network Administrator - Key		Hour		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		Hour		
<b>SUBTOTAL - LABOR</b>					<b>\$ 595,926.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)					15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 6</b>					<b>\$ 610,926.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 296,118.00</b>
<b>TOTAL VALUE - OPTION YEAR 6 (Including Optional Tasks)</b>					<b>\$ 907,044.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 7 - (03/06/2016 - 03/05/2017)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		HOUR		
Sr. Network Engineer	Engineer/Network Administrator - Key		HOUR		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		HOUR		
<b>SUBTOTAL - LABOR</b>					<b>\$ 619,745.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)					15,000.00
<b>SUBTOTAL - TRAVEL</b>					<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 7</b>					<b>\$ 634,745.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>					
SPI Analyst	Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>					<b>\$ 307,962.00</b>
<b>TOTAL VALUE - OPTION YEAR 7 (Including Optional Tasks)</b>					<b>\$ 942,707.00</b>
* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.					
<b>OPTION YEAR 8 - (03/06/2017 - 03/05/2018)</b>					
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>
Senior PMO Consultant	Project Manager - Key		HOUR		
Sr. Network Engineer	Engineer/Network Administrator - Key		HOUR		
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		HOUR		

<b>SUBTOTAL - LABOR</b>						<b>\$ 644,512.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE		\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>						<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 8</b>						<b>\$ 659,512.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>						
SPI Analyst		Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>						<b>\$ 320,274.00</b>
<b>TOTAL VALUE - OPTION YEAR 8 (Including Optional Tasks)</b>						<b>\$ 979,786.00</b>
<i>* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.</i>						
<b>OPTION YEAR 9 - (03/06/2018 - 03/05/2019)</b>						
<b>GSA SCHEDULE 70 LABOR CATEGORY</b>	<b>FUNCTIONAL LABOR CATEGORY</b>	<b>ESTIMATED QUANTITY</b>	<b>UNIT</b>	<b>(Discounted) UNIT PRICE*</b>	<b>TOTAL ESTIMATED COST</b>	
Senior PMO Consultant	Project Manager - Key		Hour			
Sr. Network Engineer	Engineer/Network Administrator - Key		Hour			
Security Specialist	Network Security Analyst (Help Desk Manager) - Key		Hour			
<b>SUBTOTAL - LABOR</b>						<b>\$ 670,274.00</b>
TRAVEL (Including G&A) - Not-to-Exceed Amount (NTE)		1	LOT	NTE		\$ 15,000.00
<b>SUBTOTAL - TRAVEL</b>						<b>\$ 15,000.00</b>
<b>TOTAL - OPTION YEAR 9</b>						<b>\$ 685,274.00</b>
<b>OPTIONAL (SOW TASKS 6.2.7 &amp; 6.3.3)</b>						
SPI Analyst		Product Specialist (Documentum) - Key (OPTIONAL)				
<b>SUBTOTAL - LABOR (OPTIONAL)</b>						<b>\$ 333,072.00</b>
<b>TOTAL VALUE - OPTION YEAR 9 (Including Optional Tasks)</b>						<b>\$ 1,018,346.00</b>
<i>* The Contractor shall charge the NRC the discounted UNIT PRICE or their actual FSS GSA hourly rate, whichever is lower during each period.</i>						
<b>CUMULATIVE TOTALS BASE &amp; OPTION YEAR 1-9</b>						
<b>CUMULATIVE TOTAL - BASE &amp; OPTION YEARS 1-9</b> (Excludes Optional SOW Tasks 6.2.7 & 6.3.3)						<b>\$ 6,021,527.80</b>
<b>CUMULATIVE TOTAL VALUE - BASE &amp; OPTION YEARS 1-9</b> (Includes Optional SOW Tasks 6.2.7 & 6.3.3)						<b>\$ 8,597,345.80</b>

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

**CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS**

**COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE**

1. CONTRACTOR NAME AND ADDRESS  <b>HUMANTOUCH, LLC</b> <b>2010 CORPORATE RIDGE, SUITE 700</b> <b>MCLEAN, VA 22102</b>	A. CONTRACT NUMBER FOR COMMERCIAL CONTRACTS OR JOB CODE FOR DOE PROJECTS (Prime contract number must be shown for all subcontracts.)  <b>NRC-DR-07-09-136</b>		2. TYPE OF SUBMISSION  <input checked="" type="checkbox"/> A. ORIGINAL <input type="checkbox"/> B. REVISED (Supersedes all previous submissions) <input type="checkbox"/> C. OTHER (Specify)
	B. PROJECTED START DATE  <b>03/06/2009</b>	C. PROJECTED COMPLETION DATE  <b>03/05/2019</b>	

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

A. DOES NOT APPLY <input type="checkbox"/>	B. CONTRACT NUMBER <b>NRC-07-07-517</b>	DATE <b>03/13/2009</b>
---	--	---------------------------

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

**SAFEGUARDS INFORMATION LOCAL AREA NETWORK AND ELECTRONIC SAFE (SLES) OPERATION AND MAINTENANCE (O&M)"**

**ORDER NO. NRC-DR-07-09-136 - ENCLOSURE 4**

5. PERFORMANCE WILL REQUIRE	A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION	NOT APPLICABLE	NATIONAL SECURITY		RESTRICTED DATA	
			SECRET	CONFIDENTIAL	SECRET	CONFIDENTIAL
	<input type="checkbox"/> YES (If "YES," answer 1-7 below) <input checked="" type="checkbox"/> NO (If "NO," proceed to 5.C.)					
1.	ACCESS TO FOREIGN INTELLIGENCE INFORMATION	<input type="checkbox"/>				
2.	RECEIPT, STORAGE, OR OTHER SAFEGUARDING OF CLASSIFIED MATTER. (See 5.B.)	<input type="checkbox"/>				
3.	GENERATION OF CLASSIFIED MATTER.	<input type="checkbox"/>				
4.	ACCESS TO CRYPTOGRAPHIC MATERIAL OR OTHER CLASSIFIED COMSEC INFORMATION.	<input type="checkbox"/>				
5.	ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION PROCESSED BY ANOTHER AGENCY.	<input type="checkbox"/>				
6.	CLASSIFIED USE OF AN INFORMATION TECHNOLOGY PROCESSING SYSTEM.	<input type="checkbox"/>				
7.	OTHER (Specify)	<input type="checkbox"/>				

B. IS FACILITY CLEARANCE REQUIRED?  YES  NO

C. <input type="checkbox"/> UNESCORTED ACCESS IS REQUIRED TO NUCLEAR POWER PLANTS.	G. <input type="checkbox"/> REQUIRE OPERATION OF GOVERNMENT VEHICLES OR TRANSPORT PASSENGERS FOR THE NRC.
D. <input checked="" type="checkbox"/> ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION.	H. <input type="checkbox"/> WILL OPERATE HAZARDOUS EQUIPMENT AT NRC FACILITIES.
E. <input checked="" type="checkbox"/> ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.	I. <input type="checkbox"/> REQUIRED TO CARRY FIREARMS.
F. <input checked="" type="checkbox"/> UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.	J. <input type="checkbox"/> FOUND TO USE OR ADMIT TO USE OF ILLEGAL DRUGS.

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

**NOTE: IMMEDIATELY NOTIFY DRUG PROGRAM STAFF IF BOX 5 A, C, D, G, H, I, OR J IS CHECKED.**

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

NAME AND TITLE  <b>Behrouz Golchane/ NSIR/PMDA Project Manager</b>	SIGNATURE 	DATE <b>2/4/09</b>
--	---	-----------------------

**7. CLASSIFICATION GUIDANCE**

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

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

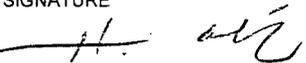
- AUTHORIZED CLASSIFIER (Name and Title)       DIVISION OF FACILITIES AND SECURITY

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

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

**10. APPROVALS**

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

NAME (Print or type)	SIGNATURE	DATE
A. DIRECTOR, OFFICE OR DIVISION  <b>Virginia Huth</b>	SIGNATURE 	DATE <b>2-4-09</b>
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY  <b>Robert Weber</b>	SIGNATURE 	DATE <b>2/5/09</b>
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements)  <b>Phyllis Bower</b>	SIGNATURE <i>for</i> 	DATE <b>2/19/09</b>

REMARKS