ORDER FOR SUPPLIES OR SERVICES

~~NRC-DR-07-09-151~~

PAGE OF PAGES: 1 | 2

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

1. DATE OF ORDER: 11-18-2008	2. CONTRACT NO. (If any): GS35F0333P
3. ORDER NO.: NRC-DR-07-09-151 MODIFICATION NO.:	4. REQUISITION/REFERENCE NO.: NSR-09-151

5. ISSUING OFFICE (Address correspondence to)
U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: H. (Eddie) Colón, Jr.
Mail Stop TWB:01-010M
Washington, DC 20555

6. SHIP TO:
a. NAME OF CONSIGNEE: U.S. Nuclear Regulatory Commission
b. STREET ADDRESS: Office of Nuclear Sec. & Inc. Response
Attn: Roya Noory, 301-415-6868
Mail Stop: T4-A57
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20555

7. TO:
a. NAME OF CONTRACTOR: HIGH PERFORMANCE TECHNOLOGIES, INC.
b. COMPANY NAME:
c. STREET ADDRESS: 11955 FREEDOM DR SUITE1100
d. CITY: RESTON | e. STATE: VA | f. ZIP CODE: 201905683

f. SHIP VIA:

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

9. ACCOUNTING AND APPROPRIATION DATA
911-15-5D1-133 I1119 251A 31X0200.911
OBLIGATE: $150,000.00 (FFS Commitment #: NSR-09-151)
DUNS #: 784366544

10. REQUISITIONING OFFICE: NSR
Nuclear Security and Incident Response

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

12. F.O.B. POINT: 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

17. SCHEDULE (See reverse for Rejections) See CONTINUATION Page

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The Contractor shall provide "SAFEGUARDS INFORMATION LOCAL AREA NETWORK & ELECTRONIC SAFE (SLES) IMPLEMENTATION" services IAW with the terms and conditions of its GSA contract, and the following attached enclosures:					
	Enclosure 1 - Price Schedule					
	Enclosure 2 - Statement of Work (SOW) w/ Attachments 1-3					
	Enclosure 3 - Additional Terms and Conditions					
	Enclosure 4 - NRC Form 187 - Contract Security and/or Classification Requirements					
	Enclosure 5 - Billing Instructions					
	BASE YEAR (11/18/2008 - 11/17/2009)				$3,117,143.00	**CURRENT CEILING**
	OPTION YEAR 1 (11/18/2009 - 11/17/2010)				$1,065,528.00	
	OPTION YEAR 2 (11/18/2010 - 11/17/2011)				$1,537,063.00	

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.
			TOTAL VALUE, INDLUDING OPTIONS $5,719,734.00
	21. MAIL INVOICE TO:		17(h) TOTAL (Cont. pages)
	a. NAME: Departement of Interior National Business Center		
	b. STREET ADDRESS (or P.O. Box): Attn: Fiscal Services Branch - D2770 7301 West Mansfield Avenue		17(l). GRAND TOTAL
	c. CITY: Denver	d. STATE: CO	e. ZIP CODE: 80235-2230
			OBLIGATED AMOUNT $150,000.00

22. UNITED STATES OF AMERICA BY (Signature)

23. NAME (Typed)
Heriberto Colón, Jr.
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE
DEC 02 2008

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

ADM001

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
11-18-2008	GS35F0333P	NRC-DR-07-09-151

ITEM NO. (A)	SUPPLIES OR SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	ACCEPTED:					
	Peter Garsevud, Director of Contracts PRINT NAME & TITLE					
	[signature] 11/18/08 SIGNATURE DATE					

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

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 REV.(4/2006)
Prescribed by GSA
FAR (48 CFR) 53.213(f)

PRICE SCHEDULE

Total, All Tasks				
BASE YEAR				
HPTi (GS-35F-0333P)			**11/18/2008 - 11/17/2009**	
GSA IT Category	**Functional Role(s)**		**Est. Hours**	**Total Est. Cost**
Senior Subject Matter Consultant	C&A Security Testing			$ 136,109.00
Senior IT Manager	Sr. Program Manager (Project Lead)			$ 61,053.00
IT Manager	Records Mgmt/Portal			$ 259,622.00
Technical Director	Program Manager; Architecture/Security			$ 575,534.00
Subtotal HPTi Labor				$ 1,032,318.00
COMTek (GS-35F-0014K)		ROUNDED	**11/18/2008 - 11/17/2009**	
GSA IT Category	**Functional Role(s)**		**Hours**	**Price**
Program Manager	Implementation Manager			$ 73,158.00
S/W Prod. Control Spec.	Project Control Specialist			$ 11,367.00
Network H/W & S/W Specialist	Net H/W & S/W Specialist			$ 74,556.00
Sr. S/W Engineer	Sr. Network Engineer			$ 289,643.00
IT Subject Matter Expert	IT SME			$ 206,101.00
Tech Writer/Editor	Doc Production Specialist			$ -
Subtotal ComTek Labor				$ 654,825.00
Subtotal Labor				$ 1,687,143.00
Hardware/Software (Not-to-Exceed Amount)		NTE		$ 1,420,000.00
Travel (Not-to-Exceed Amount)		NTE		$ 10,000.00
ODC's Subtotal				$ 1,430,000.00
TOTAL Base Year				$ 3,117,143.00
OPTION YEAR 1				
HPTi (GS-35F-0333P)		ROUNDED	**11/18/2009 - 11/17/2010**	
GSA IT Category	**Functional Role(s)**		**Est. Hours**	**Total Est. Cost**
Senior Subject Matter Consultant	C&A Security Testing			$ 16,486.00
Senior IT Manager	Sr. Program Manager (Project Lead)			$ 43,911.00
IT Manager	Records Mgmt/Portal			$ 24,019.00
Technical Director	Program Manager; Architecture/Security			$ 605,918.00
Subtotal HPTi Labor				$ 690,334.00
COMTek (GS-35F-0014K)		ROUNDED	**11/18/2009 - 11/17/2010**	
GSA IT Category	**Functional Role(s)**		**Hours**	**Price**
Program Manager	Implementation Manager			$ 55,318.00
S/W Prod. Control Spec.	Project Control Specialist			$ 8,430.00
Network H/W & S/W Specialist	Net H/W & S/W Specialist			$ 67,674.00
Sr. S/W Engineer	Sr. Network Engineer			$ 90,044.00
IT Subject Matter Expert	IT SME			$ 37,251.00
Tech Writer/Editor	Doc Production Specialist			$ 6,477.00
Subtotal ComTek Labor				$ 265,194.00
Subtotal Labor				$ 955,528.00
Hardware/Software (Not-to-Exceed Amount)		NTE		$ 100,000.00
Travel (Not-to-Exceed Amount)		NTE		$ 10,000.00
Subtotal H/W, S/W, and Travel				$ 110,000.00
TOTAL Option Year 1				$ 1,065,528.00

PRICE SCHEDULE

OPTION YEAR 2				
HPTi (GS-35F-0333P)		[redacted]	11/18/2010 - 11/17/2011	
GSA IT Category	Functional Role(s)		Est. Hours	Total Est. Cost
Senior Subject Matter Consultant	C&A Security Testing			$ 104,073.00
Senior IT Manager	Sr. Program Manager (Project Lead)			$ 43,674.00
IT Manager	Records Mgmt/Portal			$ 369,578.00
Technical Director	Program Manager; Architecture/Security			$ 610,192.00
Subtotal HPTi Labor				$ 1,127,517.00
COMTek (GS-35F-0014K)		ROUNDED	11/18/2010 - 11/17/2011	
GSA IT Category			Hours	Price
Program Manager	Implementation Manager	$		$ 57,259.00
S/W Prod. Control Spec.	Project Control Specialist	$		$ 19,204.00
Network H/W & S/W Specialist	Net H/W & S/W Specialist	$		$ 70,041.00
Sr. S/W Engineer	Sr. Network Engineer	$		$ 69,409.00
IT Subject Matter Expert	IT SME	$		$ 38,681.00
Tech Writer/Editor	Doc Production Specialist	$		$ 24,952.00
Subtotal ComTek Labor				$ 279,546.00
Subtotal Labor				$ 1,407,063.00
Hardware/Software (Not-to-Exceed Amount)		NTE		$ 120,000.00
Travel (Not-to-Exceed Amount)		NTE		$ 10,000.00
Subtotal H/W, S/W, and Travel				$ 130,000.00
TOTAL Option Year 2				$ 1,537,063.00
TOTAL VALUE, if all Options are excercised				$ 5,719,734.00

** HPTi (including team member) shall bill the NRC at the rates offered in its quote dated 10/1/2008 or the actual GSA rates (inclusive of discounts % offered in its quote dated 10/1/2008), whichever is lower.*

NRC-DR-07-09-151 Enclosure 1 - SOW

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

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

STATEMENT OF WORK

Safeguards Information Local Area Network/Electronic Safe (SLES) Production Deployment

TABLE OF CONTENTS

1. BACKGROUND 4

2. SYSTEM OVERVIEW 6

3. OBJECTIVES 7

4. SCOPE OF WORK 7

5. GENERAL REQUIREMENTS 8

6. TASKS 10

6.1 PROJECT MANAGEMENT AND INTEGRATION 10
6.2 SYSTEM REQUIREMENTS, SYSTEM ARCHITECTURE AND DESIGN REVIEW 12
6.3 EQUIPMENT PROCUREMENT (GSA FEDERAL SUPPLY SCHEDULE ITEMS ONLY) 13
6.4 EQUIPMENT CONFIGURATION AND SECURITY HARDENING 15
6.5 INFRASTRUCTURE AND SITE PREPARATION 16
6.6 SGI LAN ENGINEERING AND SYSTEM DOCUMENTATION 18
6.7 CERTIFICATION AND ACCREDITATION OF SLES FOR PRODUCTION 18
6.8 E-SAFE REVIEW FOR IMPROVEMENT AND MODERNIZATION 19
6.8.1 E-Safe Design Review for Improvement and Modernization 19
6.8.2 Migrate E-Safe Record and Document Management (RM/DM) Software 20
6.8.3 Certification and Accreditation of E-Safe 20

7. USER TRAINING AND SUPPORT TASK 21

THE CONTRACTOR SHALL REVIEW AND UPDATE THE EXISTING TRAINING MATERIALS (E.G., USER MATERIALS AND ADMINISTRATOR MATERIALS), ORGANIZE AND CONDUCT TRAINING SESSIONS WITH USERS AND ADMINISTRATORS AND REGISTER AND ISSUE TRAINING CERTIFICATES TO EACH INDIVIDUAL WHO COMPLETES THE TRAINING 21

8. PROJECT MANAGEMENT METHODOLOGY 22

9. TOOLS 22

10. PERIOD OF PERFORMANCE 22

11. PLACE OF PERFORMANCE 22

12. CONTRACTOR PERSONNEL SKILL SET REQUIREMENTS 23

13. SYSTEM SECURITY AND SAFEGUARD OF PROPRIETARY INFORMATION 24

14. STATUS MEETINGS AND PROGRESS REPORTING 26

15. GOVERNMENT FURNISHED INFORMATION 28

16. GOVERNMENT FURNISHED EQUIPMENT 28

17. TRAVEL 29

ATTACHMENTS:

Attachment 1	High Level SLES Systems Description
Attachment 2	SLES Preliminary Equipment Reference List
Attachment 3	PMM Overview

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 divisions using secured 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 compact disks (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 interested in 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. These discussions have included 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 Office of Nuclear Security and Incident Response (NSIR) is the focal point within the NRC for managing nuclear security and consolidated incident response functions. As a result, although authorized NRC staff accessing and using SGI are located throughout the agency and regions, authorized NSIR staff are the key SGI users who manage and control the large volume of SGI documents. NSIR is the sponsor of this procurement.

The scope of this procurement is limited to implementation 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). Although a future implementation of a similar system for handling classified documents has been considered, an assessment will be conducted for the development of such capability after the completion of the SLES implementation. Staff experience in technologies, administrative processes, and operations of a production system that are related to securing and controlling classified documents will be factored into that future procurement.

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 will reside on the SGI LAN; which will provide electronic management of agency SGI.

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

In Phase 1, 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 developed 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. The E-Safe SGI document repository has grown since 2005, and it continues to function in the closed room with an Interim Authority to Operate (IATO). The conditions of the IATO are described in the SLES Security Plan.

In 2006, NSIR sponsored an SGI LAN proof of concept study, which demonstrated the use and feasibility of the wireless network technology by providing access to authorized users from their desktop workstations to back-end servers with the SGI document repository. Keyboard Video Mouse (KVM) switch and Smart Card technologies provided flexibility for access and user authentication controls.

In 2006, NSIR sponsored the development of the SLES investment Business Case based on the earlier piloting 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 1.

In 2007 as part of phase 2, the SGI LAN portion of the SLES 60 user pilot was implemented. The E-Safe application continued to be developed using Documentum, a Commercial Off-The-Shelf software package, to provide full Document and Records Management capabilities and to meet the NRC security requirements for SGI documents.

In August of 2007, the Authorization to Operate (ATO) for the SGI LAN portion of the pilot was granted as a General Support System (GSS). The SGI LAN is currently being maintained in operation for NSIR pilot users in accordance to the terms of the Security Plan and the ATO approval.

The Certification and Accreditation (C&A) package for the E-Safe application has been submitted to Designated Approving Authority (DAA) for ATO grant. The ATO for E-Safe was granted in June 2008. The E-Safe application will be connected to the SGI LAN, which will mark the completion of the SLES pilot.

2. System Overview

- The SGI LAN will operate as a GSS. This network capability will provide encrypted and secure communications from thin client devices to the host servers. KVM switches are used to isolate SLES network from the NRC unsecured network at the users workstation along with strong user authentication controls through Smart Card, NRC Managed Private Key Infrastructure (MPKI), and hardened network operating systems. 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 will operate as a Major Application that will be connected to the SGI LAN. This secure document management and records management capability will provide fully featured Electronic Document Management functionality to users with secure access authorization. Management of user and group accounts will be provided as an Administration services capability.

- The SLES system must be in compliance with the NRC Management Directive 12.5, "NRC Automated Information Security Program" as the information technology (IT) security policy document.
- The access to the SLES is controlled through the following steps:

  1. Initial NRC management approval is required to provide access for each user

  2. Active Identification ID with combination of Smart Card and Public Key Information (PKI) is assigned to each user

     - Smart card and associated password is assigned
     - PKI certificate verification is performed
     - Individual E-Safe login is assigned

  3. Access Control List (ACL) functionality of Documentum will allow document owners (users) to apply granularity of access control to each document.

  4. Automatic auditing trail triggers for every event within the system.

NSIR has planned the SLES project in three development phases:

- Phase 1 included the development of the E-Safe pilot, the SGI LAN wireless network proof of concept, and the development of the SLES Business Case.

- Phase 2 includes the implementation and rollout of the SLES solution to authorized NRC headquarters and regional office users; also evaluates external access policies and procedures for access by Federal, State and Local agencies, and Licensees.

- Phase 3 includes the implementation and rollout of the SLES solution to authorized external Federal, State, and Local agencies, and Licensee representatives.

Access will be provided to resident offices as part of the licensee access. The candidate solution will be subject to the successful evaluation and coordination with Office of Information Services (OIS), the Computer Security Office (CSO) and other stakeholders.

Please refer to Attachment 1 for a high-level system description.

3. Objectives

The objectives of the SLES project are:

- To provide a secure network for authorized users to access SGI documents electronically
- Implement a secure SGI records repository in compliance with National Archives and Records Administration requirements
- Enable management (add, store, search, retrieve, collaborate, and disposition) of SGI documents in a centralized electronic document management system

To accomplish these project objectives, the primary requirements of this contract are:

- To acquire expert-level design, implementation, and operations support services for implementing solutions, appropriate application of up-to-date technologies, effective integration of infrastructure components, and cost effective operations.
- To provide for the security controls and administrative procedures and operations to protect unauthorized access and disclosure.
- To ensure compliance of the SLES capabilities with standards and guidelines required by external agencies and stakeholders at the Local, State, and Federal levels for sharing sensitive information.
- To ensure SLES capabilities and capacities are adequate for robust, reliable, stable, supportable, and secure operations to share sensitive information with a range of authorized users.

The contractor shall provide the necessary material and personnel with adequate experience and expertise to accomplish the objectives of this procurement as stated in the statement of work (SOW).

4. Scope of Work

The scope of work for this contract includes all required and necessary tasks to design and implement phased extensions for the SLES capabilities.

Phased Design and Implementation

Design and implementation consists of, but is not limited to, high level system architecture and design reviews; design of enhancements and extensions for network and systems; procurement, configuration, installation, integration, and deployment of systems and equipment (hardware and software); testing and IT security certification for new production systems; training for users and administrators responsible for managing new production systems; implementation of Disaster Recovery/backup system for Continuity of Operations (COOP) site.

The contractor shall provide, at a minimum, the described services for phased design and implementation and perform the tasks listed in this statement of work at NRC Headquarters in Rockville, Maryland. These will meet the agency requirements for the Project Management Methodology (PMM). Networking and remote user support during development and production deployment shall be provided to users at NRC Headquarters, Regions, States, Federal, and Licensee plants.

5. General Requirements

- Because of the relationship of the SLES to incident response functions in the NRC Operations Center, during deployment there may be a requirement for exceptional SLES support services during a 24 hour, 7 day a week (24/7) basis. All exceptional SLES service requests, whether though a telephone call or email or some other means of communication must be responded to by the contractor within a 60-minute timeframe from the time the service request was received.

- Under this SLES design and development contract, the contractor shall:

    - Adhere to NRC Safeguards policies and procedures to ensure protection and control of sensitive Safeguards documents. NRC MD 12.6 contains the protections for paper Safeguards documents. SLES Administration and Operations procedures contain the protections for the electronic Safeguards documents.

    - Enforce system controls and procedures which restrict user access to the SLES system to authorized users and protect against breaches or unauthorized access to sensitive documents.

    - Enforce SLES physical controls and procedures which restrict physical access to the SLES hardware and software to authorized users and protect against breaches or unauthorized access to SLES systems and equipment.

    - Report all security incidents and potential breaches or unauthorized access to the SLES designated Information System Security Officer (ISSO).

    - Ensure that all SLES media and output (i.e, CD copies, printed hard copy, etc.) are properly marked, controlled, and stored per NRC Management Directive 12.6 and the SLES Administration and Operations procedures.

- Ensure that the authorized SLES users' accounts are maintained up-to-date with new users added, and users who are no longer authorized removed from the SLES user group.

- The contractor shall not attempt to:

  - Bypass or inactivate any SLES security mechanisms; any changes to the SLES security mechanisms must be coordinated and approved by the SLES ISSO and only in effect for the restricted, specified timeframe.
  - Introduce or use software, firmware, or hardware that is not an approved component of the SLES; the effect of unapproved use is in violation of the SLES Security Plan and a security violation.

  - Bypass the approved roles and privileges that are defined for the SLES System and enforced by the SLES System Administration procedures; this may result in unauthorized access and is a security violation.

- The contractor shall train the staff assigned to this contract in IT security aspects and controls for the operating systems, devices, and applications used in this system

- 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) throughout the life of the contract. 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.

- The contractor personnel shall maintain awareness of the NRC Safeguards policies and procedures in MD 12.6 and the controls for electronic Safeguards documents which are described in the SLES Systems Administration and Operations documentation. The contractor shall maintain and update documentation as requested by the NRC System Owner or System Owner designee to keep the protections and controls for Safeguards aligned with changes in agency policy and procedures.

- The contractor shall adhere to and follow the NRC PMM throughout the life of the contract. The contractor shall develop and update SLES documentation for the PMM, as requested by the NRC System Owner or System owner designee for current SLES investment documentation. 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 3, to this statement for an overview of the PMM.

- The contractor shall consult with, and comply with (as appropriate) NRC's Enterprise Architecture reference models, including the Service Component Reference Model (SRM), Performance Reference Model (PRM), Data Reference Model (DRM), and Technical Reference Model (TRM). The contractor shall also consult with NRC's IT Roadmap, to ensure that technologies proposed for SLES comply with, or do not conflict with, the Roadmap.

- The contractor shall coordinate their activities with other NRC internal offices, such as, OIS, CSO, and the Office of Administration (ADM), as requested by the NRC System Owner or System Owner designee. The contractor shall also collaborate with NRC staff and its other contractors who may be involved with related projects, such as the Agencywide Documents Access and Management System replatforming, the agency network infrastructure upgrade, the migration to Microsoft Word and enhancements to the agency Portal technologies.

6. Tasks

The primary tasks associated with this statement of work (SOW) for NRC review and approval include:

- Project Management and development of the Integration Plan
- System Requirements (SRS) and System Architecture (SA) Review
- Equipment Procurement
- Equipment Configuration and Security Hardening
- Infrastructure, Site Preparation, Network Administration, and End-to-End Testing
- SGI LAN Engineering Documentation
- Security Certification and Accreditation of the SLES
- E-Safe enhancement/upgrade and its Certification and Accreditation
- Operations Enhancements, Coordination, and Integration

The contractor shall complete the tasks described below:

6.1 Project Management and Integration

The tasks described below are pre-requisite to the SLES Production Deployment Project execution.

6.1.1 The contractor shall attend a kick-off meeting that will be conducted within 5 days following contract award to introduce staff and to conduct a detailed project review. The agenda for this meeting will be agreed upon by the Project Officer and the contractor project manager prior to the meeting.

6.1.2 The contractor shall prepare and submit in writing to the NRC Project Officer a detailed Transition Plan for starting up support for the SLES Project. This document must include contractor's understanding of the general requirements, detailed approach, all tasks and deliverables, required staff and schedules for transitioning design and development support for the SLES Project to the new contractor organization.

6.1.3 The contractor shall prepare and submit in writing to the NRC Project Officer a detailed Project Integration Plan and Schedule. This is required by the NRC's PMM procedures, which detail various deliverables (artifacts), required for the development lifecycle stages (inception, elaboration, construction, and maintenance). The contractor shall develop this comprehensive Project Integration Plan with schedules, contractor staffing plan, milestones, and the start/end dates for each activity with their dependencies. The Project Integration Plan and schedule shall integrate all project activities and provide a level-5 Work Breakdown Structure (WBS).

The NRC PMM requires that a WBS for a project shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks (work packages) or groups of tasks with decisive outputs and specific measurable start and completion criteria. Each work package shall have a short duration, or shall be divided into a series of milestones whose status can be objectively measured. Each work package shall be given a start and a finish date integrated with higher-level schedules. The contractor WBS must conform to the PMM requirements and provide scheduled and budgeted level of effort to complete all tasks, identifying the resources needed to complete the work.

6.1.4 To ensure adequate Project Communications, the NRC PMM requires monthly Status Reports, Communications Reports (optional), and Earned Value Management System (EVMS) Reports. The Monthly Project Status Report is a list of project accomplishments during the month, planned activities for the next month, and issues or risks identified along with recommended mitigations. The monthly EVMS reports will be reporting work progress and calculate, track, and report the project Earned Value and identify variances in cost and schedule early on in order to mitigate the variance. The Communications Plan (optional) may be requested by the NRC Project Officer to communicate with the internal and external stakeholders.

6.1.5 To ensure proper Project Management practices are followed, the NRC PMM requires the following documents (the templates for these documents are maintained on the PMM web site; these are "living documents" that will be updated through production deployment)

- Software Development Plan
- Project Risk Management Plan, including Risk/Issues List
- Quality Assurance Plan
- Project Measurements

6.1.6 To ensure proper Production Deployment practices are completed for the system, the NRC PMM requires the following documents (the templates for these documents are maintained on the PMM web site; these are "living documents" that will be updated through production deployment).

- Deployment Plan
- Solution Release
- Installation Instructions

6.1.7 To ensure proper Change Management practices are completed for the system, the contractor shall follow NRC change control policies and procedures.

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 (CCB) which includes ISSO and SITSO.

The NRC PMM requires the following documents (the templates for these documents are maintained on the PMM web site; these are "living documents" that will be updated through the lifecycle of the system).

- Configuration Management Plan, including Repository Plan
- Change Request Forms

Deliverables to be produced under Project Management and Integration include:

Item	Deliverable	Estimated completion Weeks from Award
1	Project Kick-off	1
2	Transition Plan	2
3	Project Integration Plan and Schedule	4
4	Project Status Report	monthly
5	Project Management artifacts *	4
6	Production Deployment artifacts *	6
7	Change Management artifacts *	6

Note: * represents existing documents that may require updates only.

6.2 System Requirements, System Architecture and Design Review

The tasks described below are required to complete design and development of the SLES production system. The tasks confirm the existing SLES Pilot design and requirements specifications and update the existing SLES Pilot documents. It is important that this task confirm the completeness and feasibility of the SLES secure Architecture and design, particularly that (1) the SLES design can be implemented into the NRC's Production Operations Environment (POE); (2) the SLES design can support a robust, reliable, effective production system; (3) the SLES design is in compliance with the agency Enterprise Architecture and is scaleable to support additional users and communications links; (4) the SLES design has the capacity for growth in document repository, user accounts, user volume and peak load, and feature enhancements.

6.2.1 The SLES Systems Requirements and SLES Systems Architecture documents were developed during the Piloting first phase of the SLES project. The contractor shall review these two existing documents and discuss recommended changes in both the SRS and SA documents with the NRC Project Officer. In accordance with technical direction from the NRC Project Officer and following guidance provided in the NRC PMM, the contractor shall update the two existing documents with the recommended changes. The Systems Requirements and Systems Architecture documents will be reviewed and approved by the NRC project team and the Project Officer once these documents are updated.

6.2.2 The contractor shall then update the Project Integration Plan and Schedule (Task 6.1.3 above) and provide the updated Plan to the NRC Project Officer for review and approval. The Project Integration Plan will include the implementation and deployment of all components (SGI LAN, E-Safe) of the SLES system.

Deliverables to be produced for System Requirements and System Architecture Review include:

Item	Deliverable	Estimated completion Weeks from Award
1	Revised SLES System Requirement Specification, Version 2.0	4
2	Revised SLES System Architecture/Design document, Version 2.0	6
3	Revised SLES Project Integration Plan and Schedule, Version 2.0	8

6.3 Equipment Procurement (GSA Federal Supply Schedule items only)

The tasks described below are required to complete the acquisition of equipment needed to implement the SLES design approved above (Task 6.2). The tasks ensure that all necessary equipment (HW/SW) for production deployment of SLES is appropriately procured.

- As input to this task, the NRC Project Officer will provide to the contractor a preliminary short list of equipment that was used for the SLES Pilot (Attachment 2). This preliminary list is considered only informational and for reference. The contractor shall independently determine and recommend the equipment procurement needed to implement the revised SLES design. The preliminary list includes existing software licenses and manufacturer maintenance/service agreements for the current SLES Pilot system. The contractor shall consider these existing licenses and service agreements in developing the revised procurement list. All hardware and software shall be upgraded/refreshed to ensure appropriate maintainability and IT security controls. Hardware and software should not be allowed to become unsupported or insecure.

6.3.1 The contractor shall develop a comprehensive list of needed software and hardware by identifying all known software, hardware, and equipment requirements. At a minimum, the contractor shall include in the comprehensive list all special configuration requirements, potential manufacturers/vendors, and costs estimates for acquisition. The contractor shall include in the comprehensive list only licensed software; optionally, the contractor may develop a secondary list of proposed public domain, shareware, or freeware software. Because of security risks, this secondary list must be reviewed and approved (in writing) by the NRC Designated Approving Authority (DAA) before items may be considered for acquisition. Proof of software licensing is a concern for government use and must be factored into the procurement planning. The contractor will include in the comprehensive list all software, hardware, and equipment, such as servers, networking equipment (switches, wireless controllers, encryption devises, etc.), backup system equipment for COOP, users desktop and Kiosk equipment (terminals, Smartcard readers, KVM, peripheral devises, etc.), Operating System and other software, and all required use licenses.

- The contractor shall provide a comprehensive list of equipment for procurement to the NRC Project Officer for review and approval (written approval). The NRC Project Officer will develop the Request for Procurement Action, attach the approved comprehensive list for procurement, and submit to the OIS for their approval before the procurement process is initiated. Under the guidance of the NRC Project Officer, the contractor shall make any

needed updates or revisions to the comprehensive list for procurement based on the OIS review and follow-up discussions.

6.3.2 Under the guidance of the NRC Project Officer, the contractor shall revise the Project Integration Plan and Schedule to reflect timing for the various procurements in the comprehensive list.

6.3.3 The contractor shall procure all the software, hardware, equipment, tools, services listed on the approved comprehensive list for procurement. The contractor shall coordinate with the NRC Project Officer to execute the procurements based on the revised Project Implementation Plan and Schedule.

6.3.4 The contractor shall manage the entire procurement process from requesting competitive quotations from at least three approved sources and placing orders to the vendors to delivery, reception, and deployment of the equipment. **All HW/SW purchases by the contractor are subject to prior written approval by the NRC Project Officer and the NRC Contracting Officer.** The NRC/ADM Division of Contracts will provide the necessary assistance and guidance to the contractor on the acquisition. This task includes management of the entire procurement process from requesting competitive quotations from at least three (or sole-source justifications and price reasonableness) GSA FSS approved sources and placing orders to the vendors to delivery, reception and deployment of the equipment. All equipment procurement orders by the contractor are subject to **prior** written approval of the NRC Project Officer and the NRC Contracting Officer. The NRC DC will provide the necessary assistance and guidance to the contractor on the acquisition.

6.3.5 The contractor shall conduct quality inspection of delivered equipment to ensure completeness and quality of equipment, including reconciliation against the comprehensive list for acquisition. The contractor shall provide the NRC Project Officer a Validation Report which confirms receipt of individual components in working condition. The contractor shall review with the NRC Project Officer any problems or faults in equipment delivered; with approval of the NRC Project Officer, the contractor shall return faulty equipment and coordinate replacement by the vendor.

Deliverables to be produced for Equipment Procurement include:

Item	Deliverable	Estimated completion Weeks from Award
1	Comprehensive list of needed HW/SW for the production deployment of the SLES.	7
2	Revise SLES Project Integration Plan and Schedule (optional)	7
3	Procurement of equipment (HW/SW) on the Comprehensive List for production deployment.	Starting from week 12 spread out as needed
4	Equipment delivery inspection/validation report.	Starting from week 13

6.4 Equipment Configuration and Security Hardening

The tasks described below are required to complete proper preparation and security processing for all equipment that was procured (Task 6.3.3 above). The tasks ensure that all SLES production system equipment, hardware and software, is properly configured and hardened in compliance with all NRC security policies and procedures for handling sensitive systems and SGI. The SLES security categorization is determined to be HIGH.

The configurations and hardening specifications are described in the SLES Security Plan, which must be updated and approved before this task starts. The SLES Security Plan specifies security controls and procedures. The security hardening must meet the requirements outlined in the updated SLES Security Plan.

6.4.1 The contractor shall review the current SLES Security Plan, which includes equipment configuration specifications and security hardening procedures for the SLES Pilot system. The contractor shall consider whether changes will be needed to the existing and new equipment configurations or hardening to ensure adequate security. The contractor shall discuss recommended changes and revisions with the NRC Project Officer. Under the guidance of the NRC Project Officer, the contractor shall make any needed updates or revisions to the SLES Security Plan. The revised SLES Security Plan will be submitted to the SLES ISSO for review and approval (written approval). Under the guidance of the NRC Project Officer, the contractor shall make any further revisions needed based on the ISSO review and follow-up discussions.

6.4.2 The contractor shall review and revise the SLES Configuration Management documentation (see Task 6.1.7 above). The contractor shall discuss recommended changes and revisions with the NRC Project Officer. Under the guidance of the NRC Project Officer, the contractor shall make any needed updates or revisions to the configuration specifications in the SLES Configuration Management documentation to ensure that all equipment is hardened to meet the Agency's security standards for a high sensitive system, and the SLES Security Plan.

6.4.3 (Optional) The contractor shall revise the Project Integration Plan and Schedule, if needed, to adjust to revisions in work scope and schedule for configuring and hardening equipment.
6.4.4 The contractor shall configure and harden equipment, per schedule in Project integration Plan. This includes existing Pilot equipment and newly procured equipment.

The deliverables for this task include:

Item	Deliverable	Delivery weeks from Award
1	Review and Revise SLES Security Plan	28
2	Review and Revise SLES Configuration Management documentation	28
3	Revise Project Integration Plan and Schedule, if needed	28
4	Harden SLES equipment (both existing and new equipment) to meet revised SLES Security Plan specifications	Per Project Schedule

6.5 Infrastructure and Site Preparation

The contractor shall conduct an analysis of the SLES infrastructure requirement and produce a detailed Installation Plan for its implementation. This task includes the analysis, planning and assistance in the implementation of the required infrastructures and site preparation for current and planned NRC HQ buildings and each of the four NRC's regional offices. All work associated with this task related to NRC facilities must be approved by the NRC/ADM/Division of Facilities and Security (DFS).

The activities in site preparation are dependent on congruent work by OIS and its contractors. OIS will need to install the backbone wiring and the wireless access points (WAP's). The NRC Project Officer will coordinate with these needed activities and provide guidance to the SLES contractor on dependent site preparation activities. The NRC Project Officer will involve the SLES contractor in these discussions, as needed.

6.5.1 Installation Plan
The contractor shall produce all necessary installation plans and documents for the implementation of the infrastructure and site preparation (current and planned NRC buildings). Space planning for each site (buildings and floors) including the required space for the servers and other backbone system equipment, the backup and development system, on-site equipment storage and the kiosks, are part of this task. The contractor shall ensure that all site preparation and infrastructure plans complies with the Agency's physical security controls.

6.5.2 Headquarters Site
The contractor shall: (1) perform the necessary wireless surveys to determine the locations for the WAP's (current and planned NRC buildings), (2) develop installation plans (including wiring diagrams) for the wireless network components, (3) coordinate movement of equipment from the storage site to the HQ buildings,
(4) support the NRC and other contractors in wiring tasks. The contractor shall also make recommendations and specify the physical space requirements (user desktop equipment, server room, kiosks and other needed equipment locations) for system deployment in the HQ buildings.

6.5.3 Regional Sites (Regions I through IV
The contractor shall: (1) perform the necessary wireless surveys to determine the locations for the WAP's (current and planned NRC buildings), (2) develop an installation plan (including wiring diagrams) for the wireless and wired network components, (3) coordinate movement of equipment from the storage site to the regional sites, (4) support the NRC and it's contractor in wiring tasks.

The contractor shall also make recommendations and specify the physical space requirements (user desktop equipment, space for the servers and other system equipment, kiosks and storage) for system deployment in the regional office buildings.

6.5.4 End-To-End Testing
Once the infrastructure installation is complete in each of the locations (building floors), the contractor shall perform all required tests and inspections to ensure that the infrastructure is functional and site preparations are according to the plans.

- The purpose of the end-to-end testing is to detect and resolve problems early on; and that the infrastructure setup and site preparations are complete for a production release. The

contractor should plan for regression testing scripts that will be utilized throughout the lifecycle and future enhancement and updates to the SLES system. Testing for wireless SGI WAP bleed outside of approved facilities must include NRC leased buildings where SLES would be installed and the regional offices and must be part of the required system and infrastructure test plan. Minimal bleed outside the buildings is important for reducing residual security risk. Test results should confirm the bleed is not more than 10-15 feet outside approved buildings.

The contractor shall comply with the NRC PMM requirements for systems implementation, including testing requirements. Because the SLES production system processes SGI, all development and testing of the systems shall be performed on a network separated and isolated from the NRC operational network and the Internet.
In addition, the development and testing components and network must comply with all NRC security policies and procedures for a high sensitivity system.

Item	Deliverable	Estimated completion Weeks from Award
1	Site Analysis/ Infrastructure requirement document for the HQ's	10
2	Site Analysis/ Infrastructure requirement document for the regional offices.	16
3	Wireless Site Survey	18
4	Installation Plan for the WAPs, controllers and switches for each of the buildings and floors of the HQ.	20
5	Functional and Security Test Report of the system and infrastructure in the HQ	24
6	Installation Plan for the WAPs, controllers and switches in the regional offices	48
7	Functional and Security Test Report of the system and infrastructure in the regional offices	52
8	Functional and security test plans for system external access implementation.	100
9	Functional and security test report on the system external access implementation.	110

6.6 SGI LAN Engineering and System Documentation

This task ensures that all required engineering and system documents for components of the SLES (SGI LAN and E-Safe) are reviewed and, if necessary, updated. The contractor shall keep all system documentation up to date.

Existing SGI LAN and E-Safe engineering and system documents developed during Pilot phase of the project will be available for the contractor to review and update as necessary. Additional or other engineering documents may need to be created for the system C&A in production.

The deliverables for this task include:

Item	Deliverable	Estimated Completion Weeks from Award
1	Annotated document outlines documents below	33
2	SGI LAN and E-Safe Design Specifications (Physical / Layout)	33
3	SGI LAN and E-Safe Configuration Management Plan	36
4	SLES Users Guide update	40
5	SLES Desktop User Reference	40
6	SLES System Administrators Guide update	32
7	SGI Network Administrators Guide	33
8	SGI LAN and E-Safe Thread Analysis Document (s)	33

Note
The document in the table shown above, called, "SGI Thread Analysis," is a low-level engineering document. It will describe all of the system inputs and outputs (I/O) and all of the details about the system configuration and communication links. This document also describes any baseline environment variables, operating system parameters and system processes.

6.7 Certification and Accreditation of SLES for production

This task ensures that the SLES obtains the required ATO as it rolls out to all users at the NRC Headquarters buildings, the regional offices and made accessible by other authorized users from the Federal, States and local offices and licensees as part of the system production deployment. However it is expected that the contractor will be required to prepare complete C&A packages for submission during the course of this contract execution. An independent tester (an OIS contractor) shall perform the Security Test and Evaluation (ST&E), and contingency testing on the system as required for the certification and accreditation of sensitive systems. The SLES has been categorized with a FIPS 199 sensitivity of HIGH. The Contractor shall address and comply with all National Institute of Standards and Technology 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.

The contractor shall support the NSIR and its contractors in its efforts to certify and accredit the SLES under FISMA as a High Impact General Support System and the E-Safe as a Major Application connected to the SGI-LAN. Deliverables for Certification and Accreditation of the SLES in production shall 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.
This effort will also require the contractor to attend meetings and prepare presentations, memorandums and meeting minutes as needed.

The deliverables for this task shall include the following:

Item	Deliverable	Estimated Completion Weeks from Award
1	Updated SGI LAN and E-Safe Security Categorization Package if required.	37
2	Updated SGI LAN and E-Safe Risk Assessment	39
3	Updated SGI LAN and E-Safe System Security Plan	40
5	SGI LAN and E-Safe Contingency Test Plan	39
7	SGI LAN and E-Safe Contingency Test Report	40
9	SGI LAN and E-Safe ATO renewal Package	40

6.8 E-Safe Review for Improvement and Modernization

The contractor shall review and analyze the performance and functionality of the existing E-Safe system and its documentation, and interview E-Safe stakeholders to gather requirements for improving and modernizing E-Safe.

6.8.1 E-Safe Design Review for Improvement and Modernization

This task supports requirements review and the design and implementation of the required databases or improvement in the E-Safe to meet user requirements. The contractor shall analyze the existing E-Safe and its documentation, conduct interviews with E-Safe users, and collect requirements for changing or improving the E-Safe. This task may include analysis and development of management methods for monitoring and controlling external users' access to SGI.

The contractor shall document and submit recommended technical solutions to meet user specifications. The document must provide a detailed technical discussion about each proposed solution. This report should also rank each solution from most to least viable in terms of functionality applicability and cost. If the recommendations are approved by NRC, NRC would implement the solution via a contract modification.

The deliverables include:

Item	Deliverable	Estimated Completion Weeks from Award
1	E-Safe requirement analysis and specifications	56
2	Recommended Technical Solutions Document	60
3	Proposed implementation plan including cost and schedule	60

6.8.2 Migrate E-Safe Record and Document Management (RM/DM) Software

The contractor shall analyze and identify all of the tasks necessary to upgrade the E-Safe RM/DM software in alignment with the agency standard next generation Enterprise Content Management System (ECMS). If required, the contractor shall produce a detail plan and execute the system upgrade based upon the plan developed. This effort may also include data migration from the current E-Safe to the production version.

The deliverables include:

Item	Deliverable	Estimated Completion Weeks from Award
1	E-Safe ECMS RM/DM analysis document for migration	60
2	E-Safe Migration Plan	62
3	Updated E-Safe Users Guide	64
4	Update Users Reference Guide	64
5	Updated E-Safe Configuration Control document	64

6.8.3 Certification and Accreditation of E-Safe

This task supports the NRC's effort to gain certification and accreditation for the E-Safe as a Major Application in its production version. This task may be required as a result of the execution of E-Safe Record Management/Document Management software package to NRC's latest standard. The required level of effort for this task will not be significant. Also, included in this task is the review and, if necessary, update of E-Safe engineering documents for the certification and accreditation. The contractor shall work with NRC staff to obtain C&A for the E-Safe production version. This includes reviewing and updating of all required FISMA artifacts.

The deliverables include:

Item	Deliverable	Estimated Completion Weeks from Award
1	Updated E-Safe engineering documentation	64
2	E-Safe Security Categorization Package	64
3	E-Safe Risk Assessment	66
4	E-Safe System Security Plan	66
5	E-Safe Security Test and Evaluation Plan	68
6	E-Safe Contingency Test Plan	68
7	E-Safe Security Test and Evaluation Report	70
8	E-Safe Contingency Test Report	71
9	E-Safe Plan of Actions and Milestones	71
10	E-Safe ATO Package	73

7. User Training and Support Task

The contractor shall review and update the existing training materials (e.g., user materials and administrator materials), organize and conduct training sessions with users and administrators and register and issue training certificates to each individual who completes the training.

Because the Safeguards information is of high sensitivity and will require both users and administrators to observe the controls and protections which are described in the SLES Security Plan, the contractor will need to develop a separate guide and training document that ensures awareness of (1) access authorization policies and procedures; (2) responsibilities and behaviors needed to protect the Safeguards information; (3) reporting for breaches or unauthorized release of Safeguards information; (4) responsibilities for "decommissioning" or "deactivating" a user account and/or Safeguards information from the system.

Training sessions shall be provided in a classroom setting at NRC Headquarters and the regional offices. Training classes will be available for a maximum of twenty individuals per session. In addition to classroom training, the contractor shall provide hands-on training and user support to NRC staff as needed.

This task ensures that all current and new users in the headquarters, regional offices and other locations are appropriately trained to use SLES and are aware of the procedures and policies related to its use and operation. This task also includes training users on the Record Management/Document Management tool.

The deliverables for task 7 include:

Item	Deliverable	Estimated Completion Weeks from Award
1	User and Administrator Training Material	45
2	Updated user Desktop Reference	45
3	Updated SLES Security Plan for Users and Administrators	40
4	Training Sessions and Support Briefings	45
5	Data Transfer Training Material	45
6	Reports on Training	50

8. Project Management Methodology

This contractor shall adhere to the NRC 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 Overview, Attachment 3, to this statement for an overview of the PMM.

9. Tools

This project requires the contractor to use the Rational Enterprise Suite throughout the life of the contract. The NRC will provide the software on each of the contractor's Government provided desktops at NRC Headquarters. This suite of tools, which consists of RequisitePro, ClearCase, ClearQuest and Test Manager, will be used for performing requirements management, configuration management, change management, and test management. For more information on these tools, please see the IBM website at http://www-306.ibm.com/software/rational/.

10. Period of Performance

The period of performance of this task order is **November 18, 2008 through November 17, 2009** with two, one-year option periods.

11. Place of Performance

The Place of Performance for this project will be at:
U.S. Nuclear Regulatory Commission
Headquarters
11545 Rockville Pike

Rockville, MD 20852

12. Contractor Personnel Skill Set Requirements

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

- Extensive experience and knowledge of network design, security, wireless communications and wi-fi technologies and devices.
- Extensive experience in project management (Project Management Professional certified).
- Experience with designing, implementing, and testing similar secured systems .
- Extensive experience in program/system analysis, design, development, and deployment techniques for information technologies and secure network distributed systems
- Experience with Portal design and implementation and configuration
- Extensive experience with and knowledge of FISMA and application certification and accreditation
- Experience with developing administration and operations support procedures for secure wireless networks and document management systems
- Experience with training users, network, and systems administrators
- Experience with designing and implementing Enterprise Content Management systems to include records and document management tool, Documentum.

The contractor shall possess knowledge and experience in 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 requirements regarding implementation of 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

- Federal Information Security Management Act 2002
- Section 508 Compliance
- NRC Management Directive 12.5 (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 with, coordinate, and collaborate with security experts within the NRC OIS to ensure that the SLES production system follows the NRC security standards and meets the compliance requirements with security regulations.

13. System Security and Safeguard 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.

Additionally, the contractor shall comply with the following security requirement:

- All system modifications must comply with NRC security policies and procedures for a high sensitivity system, as well as federal laws, guidance, and standards to ensure FISMA compliance.

- 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 (SUNSI) 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 Contracting Officer's Technical Representative (COTR), the Senior IT Security Officer (SITSO), 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 level.

- 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.

- 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.

- 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 Accident Sequence Precursor (ASP), Hypertext Preprocessor (PHP), or Java Server Pages (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 that 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.

14. Status Meetings and Progress Reporting

Contractor shall schedule, prepare and conduct weekly project status meetings with the NRC SLES project management team during which progress and other project related issues are presented and discussed. Contractor shall produce minutes of each meeting and shall submit them within three days after each meeting to Project Officer for concurrence.

Contractor shall document/produce meeting minutes for other project related meetings as requested by the NRC staff and other project stakeholders.

14.1 Monthly Technical Progress Report

Contractor shall also provide a monthly Technical Progress Report to the NRC Project Officer and the Contracting Officer by the 10th day of each month. Additional types of status reports may also be required and will be requested by the NRC Project Officer on an as needed basis. The monthly Technical Progress Report provided shall contain a summary of the work performed for each task during the reporting period, include the appropriate statistics and plans for the next reporting period and provide a discussion about the overall project plan, problems or issues, and any proposed corrective actions with an analysis of the impact on other tasks within the scope of this statement. Issues that may affect cost and schedule must be reported to the NRC contract officer and the project officer within three days of discovery, followed by a mitigation plan based on a mutually agreed schedule. The report shall also contain a status of the projected ceiling costs, hourly/rate expenditures by resource during the reporting period, cumulative expenditures to date, funds obligated to date, a balance of the funds required to complete the order and Earned Value Management (EVM) measurements for contractor schedule and costs.

14.2 Earned Value Management Reporting

Using EVM on IT projects improves project planning, execution and promotes effective oversight.

The Contractor shall report earned value consistent with the Section A-11, Part 7 of the ANSI Standard 748. Schedule variance data submitted shall provide visibility into root causes and establish corrective actions to project completion within established task order schedule. All EVM data shall be provided in tabular and graphical formats to communicate cost variance and schedule status, as well as the technical completion status of the project relative to the Performance Measurement Baseline.

EVM data shall be collected using a Level 5 Work Breakdown Structure (WBS). The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall have a short duration, or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and can be integrated with higher-level schedules.

The Contractor shall collect and report on each of the following measures:
Performance Measurement Baseline (PMB)
Budgeted Cost of Work Scheduled (BCWS)
Actual Cost of Work Performed (ACWP)
Budgeted Cost of Work Performed (BCWP)
Cost Variance (CV) – The numerical difference between the earned value (BCWP) and the actual cost (ACWP).
CV = BCWP – ACWP.
Schedule Variance (SV) - An indicator of how much a program is ahead of or behind schedule.

SV = BCWP – BCWS.
Cost Performance Index (CPI) – The cost efficiency factor representing the relationship between the actual cost expended and the earned value.
CPI = BCWP/ACWP.
Schedule Performance Index (SPI) – The planned schedule efficiency factor representing the relationship between the earned value and the initial planned schedule.
SPI = BCWP/BCWS.
Budget at Completion (BAC) – The sum total of the time-phased budget.
Estimate to Complete (ETC) – A calculated value, in dollars or hours that represents the cost of work required to complete remaining project tasks.
ETC = BAC – BCWP.
Estimate at Complete (EAC) – A calculated value, in dollars or hours that represents the projected total final costs of work when completed.
EAC = ACWP + ETC.
The Contractor shall calculate Earned value credit as a binary value, with 0 percent being given before task completion and 100 percent given when completion of each work unit is validated by the NRC Project Officer. The Contractor shall establish specific measurable exit criteria for each task to simplify tracking of task completion, and thus credit the earned value of the task to the project so that the earned value of the project at any given point in time is obtained by "simple math" rather than by subjective assessment.

15. Government Furnished Information

The following information shall be provided by the NRC during the performance period of this contract:

- E-Safe System documentation
- SGI SLES System Architecture Document, Version 1.0
- SLES Business Case (specific components as it pertains to the contractor's tasks)
- SLES approved Security Plan
- NRC PMM documentation (artifacts specifications)
- NRC FISMA documentation (certification and accreditation artifacts specifications)
- NRC Pilot SLES system documentation

16. Government Furnished Equipment

The following resources shall be provided by the NRC:
The NRC will provide authorized contractor personnel with appropriate access to the NRC Rockville, MD building and the applicable spaces for installation and storage of the SLES equipment.

For the duration of the project, the NRC will provide four standard workstations with a standard NRC PC and a monitor at the NRC Headquarters in Rockville, Maryland. These four workstations will be used by the contractor for daily administrative tasks and will not contain project sensitive data. The workstations will have the appropriate access to required staff and data and may be in a security access controlled area. There will be an email account for each of the contractor staff

working on the project. The workstation will have internet connection, but all internet access will be monitored by the LAN system administrator.

For the duration of the project development activities, the NRC will provide access for the contractor to all necessary hardware and software which is required for the development, and testing of the SLES system. This equipment will be secured and may contain sensitive Safeguards and Safeguards related data. This equipment will be separated and isolated to a secure network environment. This equipment will reside within a security access controlled area.

The contractor shall adhere to NRC security policies and procedures related to the access and use of this equipment. The contractor shall configure and harden this equipment in compliance with all NRC security policies and procedures for a high sensitivity system.

The contractor shall be responsible and accountable for all Government furnished equipment provided under this contract and shall comply with the provisions of the FAR Government Property Clause under this contract and FAR Subpart 45.5, as in effect on the date of this contract. The contractor shall investigate and provide written notification the NRC contracting Officer (CO) and the NRC/ADM/DFS, Physical Security Branch of all cases of loss, damage, or destruction of Government property in its possession or control not later than 2 hours after discovery. The contractor must report stolen Government property to the local police and a copy of the police report must be provided to the CO and to the NRC/ADM/DFS, Physical Security Branch. All other equipment/property required in performance of this contract shall be furnished by the contractor.

17. Travel

It is estimated that up to ten (10) one-person, 2 day trips 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, Maryland.) 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 required document under Project Coordination and Integration and according to the planned schedule as part of the project pre-approved project base-line schedule.

Attachment # 1 - High Level SLES Systems Description

This document provides a high level description of the SLES system, its interfaces and the operational environment for a better understanding of what the target system is designed to accomplish.

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 will reside on the SGI LAN; which will provide electronic management of agency SGI.

The SGI LAN operates as a General Support System (GSS). The E-Safe is a Major Application which will be connected to the SGI LAN.

The network is predicated on the following core components:

1. SGI LAN host servers are maintained in a secure room.
2. Secure Wireless network infrastructure will provide encrypted and secure communications from access devices (thin clients) to the host servers.
3. Thin Client devices utilize KVM switches for authorized users to access the SGI LAN with low impact to existing unclassified PC environment.
4. Secure Regional Office Segments supported by encrypted tunnel within the NRC communications infrastructure.
5. A highly secure out-facing segment of the LAN (DMZ) shall be used for internet channel communications for external authorized users only.
6. Secure Web Services will provide portal access to remote users on encrypted channels.
7. Strong authentication controls using a combination of Smartcard, PKI and hardened network Operating System is used.

SGI LAN - Access Scenarios

The table that follows serves to illustrate several scenarios by which various authorized users may access the SGI network. The table should be used in conjunction with Figure 1: System Context Diagram to gain a high-level understanding of the system interfaces that would be put into place to access the SLES. Note that part of the NRC SLES wireless network (internal) has been implemented for approximately 60 users as part of the pilot implementation. Note: The illustration references within the table relate to the triangular markers within Figure 1:

System Context Diagram.

SLES - Access Scenarios	Users	User Action	System Response	Illustration Reference
NRC SLES Network (Wireless) - Internal	NRC Employees	Authorized NRC user will set the KVM switch to connect their keyboard, mouse, and monitor to the thin client. User then power up the SLES Thin client terminal and inserts the Smartcard in the reader to login to the SLES system.	The system will prompt the user to provide a PIN code associated with his or her Smartcard.	1, 2, 3
		The user will provide the system with a PIN code associated with their Smartcard.	The system will read and register the PIN code provided by the user. The system will then challenge the user to authenticate with a valid username and password.	
NRC Network – External	NRC Regional Offices	Authorized NRC user will set the KVM switch to connect their keyboard, mouse, and monitor to the thin client. User then power up the SLES Thin client terminal and inserts the Smartcard in the reader to login to the SLES system.	The system will prompt the user to provide a PIN code associated with their smartcard.	1, 6

		The user will provide the system with a PIN code associated with their Smartcard.	The system will read and register the PIN code provided by the user. If the PIN matches, the user will be provided access to the appropriate data and functionality.	
Internet Portal (DMZ)	External Authorized Users: NRC Employees, Federal, State Agencies, Local Government, Power Plants, Licensee sites or Key Contractors	Remote access to authorized users will be provided via a secure URL, which will point to the SLES Portal running in the DMZ.	The system will prompt the user to provide a PIN code associated with their Smartcard or token.	1, 4, 5
		The user will provide the system with a PIN code associated with their smartcard or token.	The system will read and register the PIN code provided by the user. If the PIN matches, the user will be provided access to the appropriate data and functionality.	

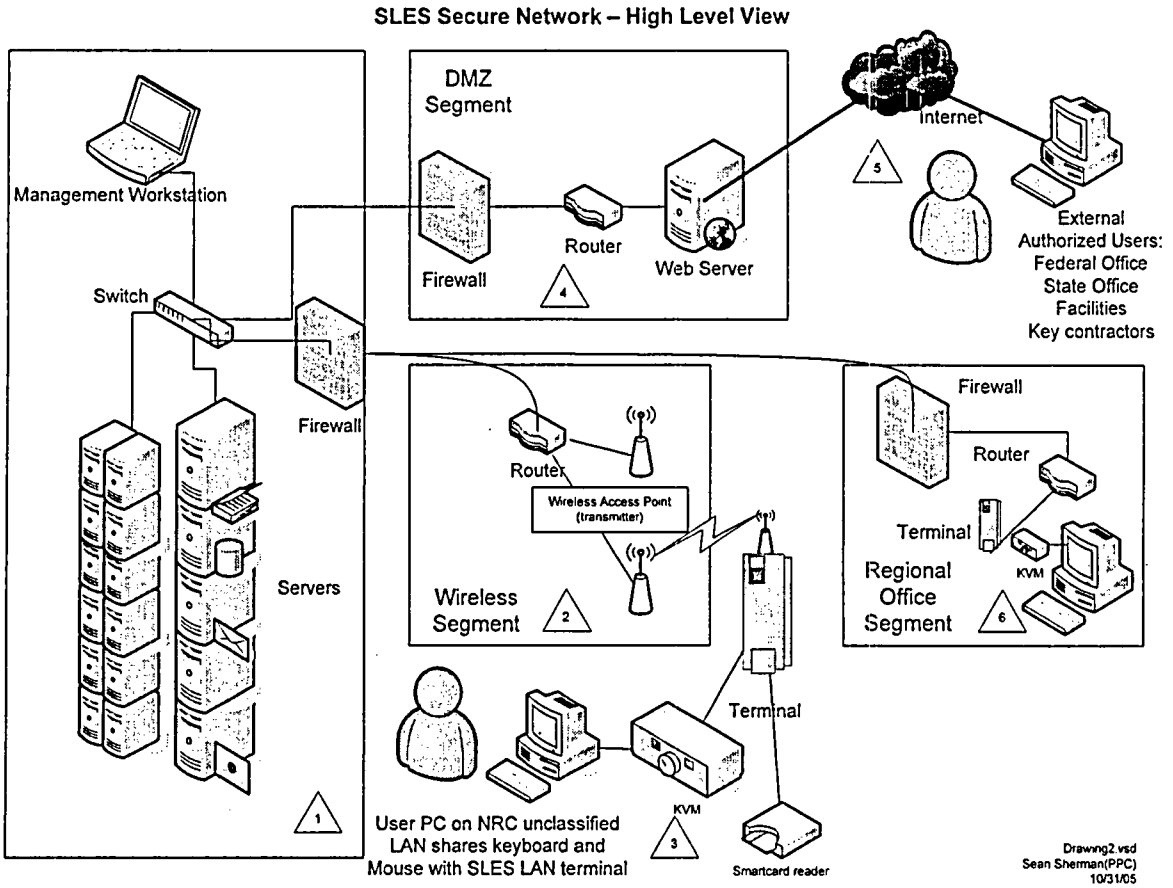


Figure 1 - System Context Diagram

1.1 Functional Capabilities

E-Safe

The E-Safe provides document management and records management features as defined in the Safeguards SLES System Requirements Specification. The significant features built into the E-Safe are:

- Document Management – document capture and scanning, search and retrieval, version control, organizing and packaging documents, reporting, workflow and approval
- Records Management – records schedules, disposition and destruction of records
- Security and Administration - user account and group management; need to know access control to documents, folders and packages for users and groups

Paper and or electronic documents are delivered to the secure room for scanning by authorized staff. Electronic files are handled in the secure room in accordance with security requirements. Select authorized Document Processing Center (DPC) personnel are the primary personnel allowed to scan, capture, and profile paper and or electronic SGI documentation into the E-Safe repository. Additionally, maintaining the documents, document repository, and document profile information is only allowed for select authorized personnel in accordance with the system security requirements. The document profile is the portion of the E-Safe repository that collects and maintains information about the related document. This information includes information such as the document title and date of entry into the E-Safe (See the Data Requirements section of the SRS for the profile definition). Further maintenance of the documents profile will be performed by other select authorized personnel such as the author and document owner.

SGI LAN

The SLES system will provide a network environment, and will include a secure portal for controlled access to E-Safe and other applications. The network must provide a robust user capacity and an electronic and physically secure environment. The network must be approved for SGI data which will require OIS approval and DAA accreditation. The key systems requirements for the network are in a table in the following section. The table was extracted from the SLES SRS documentation and reviewed in the SLES Candidate Solutions Analysis which discussed the functional capabilities, alternatives and recommendations.

1.2 System Characteristics

A Secure SGI Network will contain at the following components:

- Core components including: LAN protocol, the local area network servers providing domain, data, and application hosts, an intrusion detection system, web servers, firewalls, routers, power backup and physical access controls.
- A device on the user's desktop or at a common access terminal (kiosk) which allows access to the network. For example, a personal computer or a "thin client" terminal would fill this function.
- The transmission medium which connects the servers, data and applications to users, either on desktop or remotely. Examples of transmission technology include fiber optic cable, standard copper network cable (Ethernet category 5), or wireless RF transmission.

Privacy Considerations

There will be no information covered by the Privacy Act contained in this system

There is no PII (non-public, personally identifiable information) stored by the SLES system.

SLES Preliminary Equipment Reference List (HW/SW)

Attachment # 2

WYSE Terminals	Part Number	Brand
Wyse V90 (512 MB Flash/256MB RAM)	902094-05	WYSE
Wyse V90 (512 MB Flash/512MB RAM)	902094-21	WYSE
Wyse Device Manager (Rapport),Per Seat	730804-50	WYSE
3 yr Upgrade/Maintenance Contract, Wyse Device Mgr	730939-06	WYSE
Wireless NIC	3CRPAG175B	3Com
Avocent KVM Model MM2	2SVPUA20-001	Avocent
Avocent KVM Cables for USB Keyboards	SVUSB-6	Avocent
External Floppy	PA905U	TARGUS
External CD/RW	32885	Iomega
External DVD/RW	33173	Iomega
Power Strip (fused) – 8 Outlet	STP180	BELKIN
Fast Ethernet 100Base –TX to 100Base-FX	E-100BTX-FX-05(SC)	Transition
Enterprise Access Card Solution (CMS-ActivClient) WIN Package	EAB54WP	ACTIVIDENTITY
PCM two reader, 3 tokens	PCM 203P	ACTIVIDENTITY
ActivCard 64K smart cards -No profile-25 unit package	SC064JWA0025	ACTIVIDENTITY

Server Equipment	Part Number	Brand
PE 2850, 2.8Ghz/2MB, XEON, 800 FSB2.8Ghz/2MB Cache, Xeon, 800Mhz-r with 4GB of memory (222-3342) (with all the specifications included in the quote 302513192)	PE2850	DELL
Optiplex GX520 Small Form Factor Pentium 4 640/3.2Ghz 2M, 800FSB, HyperThreading (221-9641) (with all the specifications included in the quote 302517815)	OptiPlex GX520 SFF	DELL
17IN LCD 500:1 1280X1024 LCD1770NX-BK Black DVI/VGA USB	LCD1770NX-BK	NEC
Wireless NIC	A02517815	3COM
CISCO NETWORKING	**Part Number**	**Brand**
GE SFP, LC connector SX transceiver	GLC-SX-MM=	CISCO
Catalyst 3560 24 10/100 PoE + 2 SFP Enhanced Image	WS-C3560-24PS-E	CISCO
SMARTNET 8X5XNBD Catalyst 3560 24 10/100	CON-SNT-356024PE	CISCO
GE SFP,LC connector SX transceiver	GLC-SX-MM=	CISCO
Cisco Secure ACS 4.0 Solution: includes HW and SW	CSACSE-1113-K9	CISCO
Config. Option; CSACS 4.0 Software loaded on Cisco 1112	CSACSE-4.0-SW-K9	CISCO
SMARTNET 8X5XNBD Cisco Secure ACS 4.0	CON-SNT-CSA1113	CISCO
SW APP SUPP Cisco Secure ACS 4.0	CON-SAS-CSA1113	CISCO
SW APP SUPP Config. Option: CSACS 4X SW	CON-SAS-CSACS4.X	CISCO
4400 Series WLAN Controller for up to 12 Lightweight APs	AIR-WLC4402-12-K9	CISCO
AIR Line Cord North America	AIR-PWR-CORD-NA	CISCO
Software	SWLC4400K9-40	CISCO
SMARTNET 8X5XNBD 4402-12 WLAN Controller	CON-SNT-WC440212	CISCO
802.11ag LWAPP AP Integrated Antennas FCC Cnfg	AIR-LAP1131AG-A-K9	CISCO
AIR Line Cord North America	AIR-PWR-CORD-NA	CISCO
Power Supply	AIR-PWR-A	CISCO
Cisco 1130 Series IOS WIRELESS LAN LWAPP RECOVERY	S113RK9W-12307JX	CISCO
SMARTNET 8X5XNBD 802.11ag LWAPP AP Intg Ant FCC Cfg	CON-SNT-LAP1131A	CISCO
Fortress 7500 Secure Gateway Includes first year of maintenance	AF7500M	FORTRESS
Maintenance 7500 (3 yrs)	SS-7500-1	FORTRESS
Fortress Access Control Software (ACS)	AF-ACS	FORTRESS
Fortress maintenance & support for 1 additional year for ACS	AF-ACS-1	FORTRESS
Fortress Client Software license	FCLT-WIN	FORTRESS
Maintenance CALS (3 yrs) for 65 users	SS-CLT-WIN-1	FORTRESS

Software	Part Number	Brand
Windows 2003 Server	P73-00205	MS
Terminal Service Client (20 Licenses per package)	R19-00847	MS
MS Outlook Client CAL	381-01590	MS
SQL Server Client	359-01711	MS
MS Office Pro	269-06826	MS
Exchange Server	312-02662	MS
SQL Server 1 Processor License	228-03132	MS
Veritas BEWSSVR CPSV10.1COMBOFULL V ERLIC/24X7SPT 1YRVL E	S180498-OLE000	SYMANTEC
Veritas BackupExec - Exchange	S180618-OLE000	SYMANTEC
Veritas BackupExec - SQL	S180638-OLE000	SYMANTEC
Citrix Metaframe Presentation Server Xpe	MW2ZPSE0001	CITRIX
ECORA software	**Part Number**	**Brand**
Enterprise Windows Maintenance 1-yr	MI-EA-36 V3.X	ECORA
Auditor Maintenance - 3 yrs	MI-AM-36 V3.X	ECORA
Sessions of Rapid Remote Professional Services	PS-EA-R	ECORA

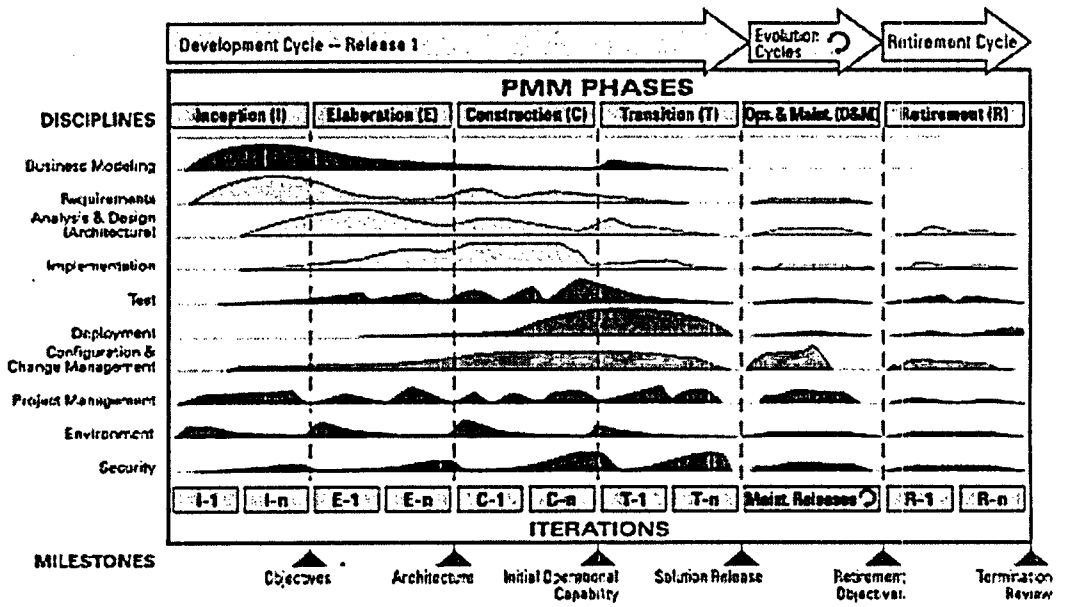
Printers	Part Number	Brand
5110cn Color Laser Printer	222-2215	DELL
511cn 500 Sheet Drawer	310-7900	DELL
USB Printer cable		DELL
Workgroup Laser Printer 521n	222-0945	DELL
521n Duplexer	310-7228	DELL
Misc.	**Part Number**	**Brand**
VIEWSONIC VA912B 19in DVI LCD Black	VA912B-4	Viewsonic

Attachment #3 - 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.

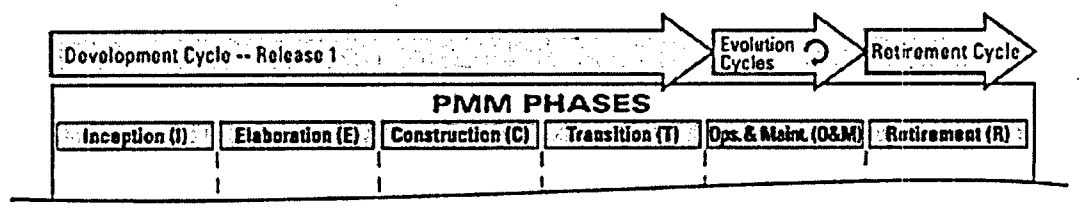
This single Management Directive includes both the policy and a configurable process with guidance, tools, and templates to support the implementation of that process. The PMM initiative is a direct response to concerns raised by agency staff to reduce the burden of IT project management. Further, PMM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

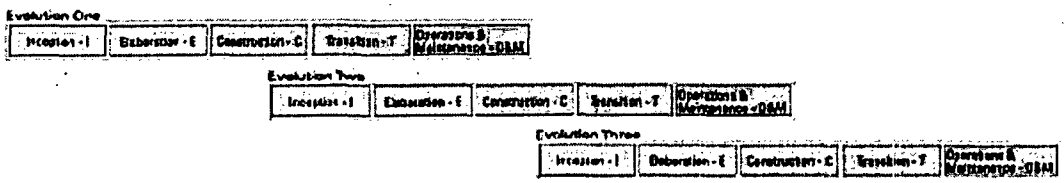
Retirement Cycle

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

NRC-DR-07-09-151 - Enclosure 3

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 contract is **$3,117,143.00**.

(b) The amount presently obligated with respect to this contract is **$150,000.00**. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the contract ceiling as specified in paragraph (a) above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this contract. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk.

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

Alternate 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**

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

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

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.
(3) Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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:

John Porter	**Project Manager**
Tom Wolf	**Senior Architect**
Len Natkin	**C&A Lead**
Marty Shoup	**Document and Records Management Lead**
George "Josh" Eisenhardt	**Deployment Manager**

Dirar Hakeem **System Architect**

Tariq Amjed **Sr. Network Engineer**

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

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

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

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

A.4 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.

(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;

(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.

A.5 2052.204-70 SECURITY (MARCH 2004)

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

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

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

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

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

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

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

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

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

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

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

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

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

A.6 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MARCH 2006)

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

A.7 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY ACCESS APPROVAL (FEBRUARY 2004)

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

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

SECURITY REQUIREMENTS FOR LEVEL I

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

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

A contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by Security Branch, Division of Facilities and Security (SB/DFS). Temporary access may be approved based on a favorable adjudication of their security forms and checks. Final access will be approved based on a favorably adjudicated LBI in accordance with the procedures found in NRC MD 12.3, Part I. However, temporary access authorization approval will be revoked and the employee may subsequently be removed from the contract in the event the employee's investigation cannot be favorably

adjudicated. Such employee will not be authorized to work under any NRC contract without the approval of SB/DFS. Timely receipt of properly completed security applications is a contract requirement. Failure of the contractor to comply with this condition within the ten work-day period may be a basis to void the notice of selection. In that event, the Government may select another firm for award. When an individual receives final access, the individual will be subject to a reinvestigation every 10 years.

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

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

SECURITY REQUIREMENTS FOR LEVEL II

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

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

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

The contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the Project Officer to the NRC SB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the

contractor in a sealed envelope), as set forth in MD 12.3. Based on SB review of the applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility under the provisions of MD 12.3. Any questions regarding the individual's eligibility for IT Level II approval will be resolved in accordance with the due process procedures set forth in MD 12.3 and E.O. 12968.

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

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

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

A.8 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.

A.9 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 5 years.

A.10 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (JULY 2006)

(a) The U.S. Nuclear Regulatory Commission (NRC) contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC contractor(s) and subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24.

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

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

A.11 2052.215-78 TRAVEL APPROVALS AND REIMBURSEMENT -ALTERNATE 1 (OCT 1999)

(a) Total expenditure for travel may **not** exceed **$10,000.00** 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-122, Cost Principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.

ENCLOSURE – 4

NRC FORM 187
(7-2008)
NRCMD 12

U.S. NUCLEAR REGULATORY COMMISSION

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

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

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS

High Performance Technologies, Inc. (HPTi)
11955 Freedom Drive, Suite 1100
Reston, VA 20190

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

NRC-DR-07-09-151

B. PROJECTED START DATE	C. PROJECTED COMPLETION DATE
11/18/2008	11/17/2011

2. TYPE OF SUBMISSION

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

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

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

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

SLES Implementation

5. PERFORMANCE WILL REQUIRE

A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION
- [ ] YES (If "YES," answer 1-7 below)
- [x] NO (If "NO," proceed to 5.C.)

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

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

C. [ ] UNESCORTED ACCESS IS REQUIRED TO NUCLEAR POWER PLANTS.

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

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

F. [x] UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.

G. [ ] REQUIRE OPERATION OF GOVERNMENT VEHICLES OR TRANSPORT PASSENGERS FOR THE NRC.

H. [ ] WILL OPERATE HAZARDOUS EQUIPMENT AT NRC FACILITIES.

I. [ ] REQUIRED TO CARRY FIREARMS.

J. [ ] 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	SIGNATURE	DATE
Roya Hoopy Behrouz Golchane/ NSIR/PMDA/IT		2/25/08

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

02/28/08

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 Virginia Huth	Virginia A Huth	02-26-08
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY Mark D. Lombard		2/28/08
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements) Phyllis A. Bower	for	11/13/09

REMARKS

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

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

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

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

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

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

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

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

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

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

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

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

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

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

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

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

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

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

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

Supersession: These instructions supersede any previous billing instructions.

R:txtselden\billing instructions LH or TM revised 2008

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 _____.

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