ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 / 23

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

1. DATE OF ORDER	SEP 27 2010
2. CONTRACT NO. (If any)	NRC-DR-33-10-342
3. ORDER NO.	T001
MODIFICATION NO.	
4. REQUISITION/REFERENCE NO.	33-10-342

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

6. SHIP TO:

a. NAME OF CONSIGNEE	U.S. Nuclear Regulatory Commission
b. STREET ADDRESS	11646 Rockville Pike
c. CITY	Rockville
d. STATE	MD
e. ZIP CODE	20785
f. SHIP VIA	

7. TO:

a. NAME OF CONTRACTOR	CGI FEDERAL INC.
b. COMPANY NAME	
c. STREET ADDRESS	12601 FAIR LAKES CIR
d. CITY	FAIRFAX
e. STATE	VA
f. ZIP CODE	220334902

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.

☒ b. DELIVERY
Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA
B&R: 010-15-5G1-348 JC: J1250 BOC: 252A
Appr# 31X0200 FFS# 10070673
Obligation $1,500,000.00 DUNS: 145969783

10. REQUISITIONING OFFICE OIS
Office of Information Services

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

12. F.O.B. POINT
Destination

13. PLACE OF

a. INSPECTION	SEE BLOCK 6
b. ACCEPTANCE	SEE BLOCK 6
14. GOVERNMENT B/L NO.	
15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	09/30/2011
16. DISCOUNT TERMS	Net 30

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The Contractor shall provide services in accordance with the attached PWS titled "Performance Work Statement for Task Order #1 - ADAMS System Support and Application Migration. PO: Gary Young 301.415.7104; gary.young@nrc.gov Total Order ceiling: $1,734,837.80 Total Obligated Amount: $1,500,000.00 Period of Performance: 9/27/2010-9/26/2011					

18. SHIPPING POINT	
19. GROSS SHIPPING WEIGHT	
20. INVOICE NO.	
17(h) TOTAL (Cont. pages)	$1,500,000.00
17(i). GRAND TOTAL	$1,734,837.80

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:

a. NAME
Department of Interior / NBC
NRCPayments@nbc.gov

b. STREET ADDRESS (or P.O. Box)
Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue

c. CITY Denver d. STATE CO e. ZIP CODE 80235-2230

22. UNITED STATES OF AMERICA BY (Signature) Pearlette Mer

23. NAME (Typed)
Pearlette Merriweather
Contracting Officer
TITLE: CONTRACTING/ORDERING OFFICER

B. PRICE SCHEDULE:

This is a labor-hour task order. Authorized labor categories and associated fixed hourly rates include:

Labor Category	Fixed Hourly Rate	Estimated Hours	Ceiling Price
Project Manager II	[redacted]	[redacted]	[redacted]
Developer II	[redacted]	[redacted]	[redacted]
Developer I	[redacted]	[redacted]	[redacted]
Security Analyst III	[redacted]	[redacted]	[redacted]
Subtotal CGI Labor		[redacted]	**$ 1,044,601.60**
Subcontracted Services			
Project Analyst - SRE	[redacted]	[redacted]	[redacted]
Principal ECM Engineer - SCS	[redacted]	[redacted]	[redacted]
Senior Architect - EnChoice	[redacted]	[redacted]	[redacted]
Subtotal Subcontractor Labor		[redacted]	**690,235.2**
Grand Total		[redacted]	**$ 1,734,836.80**

U.S. Nuclear Regulatory Commission
Office of Information Services
Performance Work Statement for Task Order 1
ADAMS System Support and Application Migration

1.0

2.0 Background

The U. S. Nuclear Regulatory Commission (NRC) ensures that the nation safely uses radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as nuclear medicine, through licensing, inspection, and enforcement of its regulations. Information associated with these endeavors are stored in and accessed from many different repositories; the primary repository is a document management system known as the Agency-wide Documents Access and Management System (ADAMS). ADAMS is discussed in detail in *Section C.4, Overview of ADAMS.*

The Office of Information Services (OIS) plans, directs, and oversees the NRC's information resources, including technology infrastructure and delivery of information management and technology services to meet the mission and goals of the agency and is the business sponsor of this effort.

The OIS Information and Records Services Division (OIS/IRSD) plans, develops, and delivers programs and services related to the storage, retrieval, protection, and preservation of NRC information in paper and electronic media. It also assists internal and external stakeholders obtain NRC information through the Public Document Room, ADAMS Support Center, the Technical Library, the File Center, the NRC internal and external Web Sites, and the FOIA and Privacy Act programs. IRSD manages a centralized system for the electronic search and retrieval of internal and external agency documents. It also develops and administers the agency information collection budget and directs the agency's records management services.

The Enterprise Content Management (ECM) Program was established within OIS/ IRSD to address agency content management needs that include, but are not limited to, content storage, eForms, search/query/discovery, retrieval, versioning/change management, records management, compliance, capture/ingest, workflow, digital signature, collaboration, security (content security and Federal Information Security Management Act (FISMA) compliance), administration, taxonomy, metadata, data quality/integrity, Personally Identifiable Information (PII) management, rendering, publishing, and enterprise reporting.

3.0 Objective

The objective of this Performance Work Statement (PWS) is to outline the required professional Information Technology (IT) Services for the NRC ECM Program. Contract services are intended to be provided primarily by IBM FileNet P8 certified and authorized subject matter expert and project management professional contractor for the purpose of providing a full range of IT services, technical expertise, and project management expertise to:

1. Ensure ADAMS operations meets applicable standards by applying Agency adopted project management methodologies;

2. Provide implementation support and re-engineering services to migrate ADAMS applications operating under IBM FileNet Content Services operating system (OS) to operate under the IBM FileNet P8 OS..

3. Maintain synchronized ADAMS Main Library (FileNet Content Services) with the FileNet P8 Main Library by operating existing synchronization routines. (see section C.5, ADAMS Libraries and Access Mechanisms);

4. Provide operations and maintenance support for the IBM FileNet Content Services OS (while it remains operational during the migration effort) and the P8 OS as well as the applications that run on each of these environments;

5. The NRC intends to use another contractor ("NRC's security contractor") to serve as the primary developer of deliverables needed for the Security Certification and Accreditation of ADAMS and related systems. The Contractor shall work with the NRC's security contractor to provide them the information they need to develop the deliverables required for the Security Certification and Accreditation of ADAMS and related systems.

4.0 Scope of Work

The Contractor shall support the Office of Information Services (OIS) / Information and Record Services Division (IRSD) according to the IDIQ Statement of Work for Solicitation No. NRC3310ADAMS

Note: Any Contractor personnel working under this task order can not take on the role of certification agent for any OIS/IRSD system. At no time is the Contractor allowed to configure an OIS/IRSD operational system.

The Contractor shall provide a full range of IT services, technical expertise, integration services, software development services, and project management. The Contractor shall furnish the necessary personnel, materials, equipment, facilities, travel, and other services required to satisfy the requirements of this PWS.

The Contractor shall perform the following tasks:

4.1 Task 1: Information Technology (IT) Project Management

The Contractor shall perform the following requirements on a firm-fixed-price per month basis:

The Contractor shall provide a full range of business and IT project management and consulting services that assist in ensuring that the IBM FileNet P8 system meets NRC standards and is performing to its defined configuration, cost, schedule, and performance specifications/capabilities. This might include performing independent technical assessments as well as supporting the development, implementation, and continuous improvement of policies, procedures, guidelines, and directives related to or impacted by the IBM FileNet P8 system. These services encompass all areas of the IT program and project management oversight including, but not limited to, issues management, enterprise architecture, information security, training, communications, organizational change, performance management, quality management, and risk management.

4.1.1 Project Plan

The Contractor shall develop a Project Plan. The Contractor shall reflect the considerations of other NRC support services areas (e.g., infrastructure, computer security, enterprise architecture, emerging business needs) in the Project Plan. The Project Plan shall define the approach to be used by the Contractor to deliver the objective of this PWS. The Project Plan shall use the Project Plan template in NRC Management Directive (MD) 2.8. The Contractor shall ensure the WBS laid out in the Project Plan adequately defines all work necessary to meet the requirements of this task order. The Project Plan shall be baselined and used as the basis for Earned Value Management calculations and change management.

The Project Plan shall be readable by Microsoft Project 2007 or later. The Contractor shall provide an updated Project Plan to the Project Officer on a monthly basis and shall be delivered to them in conjunction with the Monthly Status Report.

4.1.2 Configuration Management

The Contractor shall develop and maintain a Configuration Management (CM) Plan. The CM Plan shall include a schedule that lists items to be under CM control during the configuration, integration, testing, implementation, re-engineering, and migration of any IBM FileNet P8 platform products and any non-IBM third-party Enterprise Content Management (ECM) software that is procured (by the NRC, not the Contractor) during the period of performance of this task order. The NCR will provide a list of all software the contractor is responsible for keeping under configuration control.

4.1.3 Risk Management

The Contractor shall develop and maintain a Risk Management (RM) Plan. The RM Plan shall, at a minimum: 1) identify risks and provide a mitigation plan for critical path items in a timely fashion and 2) present a process for implementing proactive risk management as part of the overall management of the project. This RM Plan shall serve as a basis for identifying alternatives to achieve cost, schedule, and performance goals, assist in making decisions on budget and funding priorities, provide risk information for scheduling decisions, and allow monitoring of the effectiveness of the project. The RM Plan shall describe methods for identifying, analyzing, prioritizing, and tracking risk drivers; developing risk-handling plans; and planning for adequate resources to handle risk.

4.1.4 Earned Value Management

The Contractor shall apply Earned Value Management (EVM) techniques and report earned value consistent with: 1) the American National Standards Institute /Electronic Industries Alliance (ANSI/EIA) 748-A Standards, which provide a set of best business practices for establishing and applying an integrated management system with coordination of work scope, schedule, and cost objectives and application of earned value methods for program or enterprise planning and control and 2) NRC Management Directive (MD) 2.8. The Contractor's schedule of variance data submitted shall provide visibility into root causes and establish corrective actions to achieve project completion within established task schedule. The Contractor shall provide all EVM data 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.

The Contractor shall collect EVM data using a Level 3 WBS (equivalent to 1.1.1) and include a definition of the work to be conducted broken down 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 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 able to be integrated with higher-level schedules.

The Contractor shall report on each of the following measures:

1. Performance Measurement Baseline (PMB)
2. Budget Cost of Work Scheduled (BCWS)
3. Actual Cost of Work Performed (ACWP)
4. Budgeted Cost of Work Performed (BCWP)
5. Cost Variance (CV) – The numerical difference between the earned value (BCWP) and the actual cost (ACWP). CV = BCWP – ACWP.
6. Schedule Variance (SV) - An indicator of how much a program is ahead of or behind schedule. SV = BCWP – BCWS.
7. Cost Performance Index (CPI) – The cost efficiency factor representing the relationship between the actual cost expended and the earned value.
   CPI = BCWP/ACWP.

8. Schedule Performance Index (SPI) – The planned schedule efficiency factor representing the relationship between the earned value and the initial planned schedule. SPI = BCWP/BCWS.
9. Budget at Completion (BAC) – The sum total of the time-phased budget.
10. 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.
11. 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.

4.1.5 Monthly Status Reports

The Contractor shall submit an electronic version of a Monthly Program Status Report to the Project Officer according to Table 1 - Deliverables under Task 1. At a minimum, the following items shall be included in each status report:

1. Summary (accomplishments, overall status of all tasks)
2. Financial (include staff utilization)
3. Schedule (updated monthly)
4. Planned Activities
5. Report on the EVM data as outlined in Section C.10.1.4
6. Issues and Concerns (include risk and mitigation strategies)
7. Updated Project Plan
8. Action Items

4.1.6 Office of Management and Budget (OMB) Exhibit 300 for ADAMS

The Contactor shall provide support for completing OMB Exhibit 300 exercise for ADAMS. Required Contractor activities include contacting the Project Officer to obtain planning, budgeting, and acquisition data and information for the Primavera ProSight portfolio management system for timely Exhibit 300 submission by the NRC to the Office of Management and Budget.

Table 1 - Deliverables under Task 1 include:

Deliverable	Due Date (No Later Than)
Draft Project Plan	10 days after task order award
Final Project Plan	30 days after task order award
Configuration Management Plan	30 days after task order award
Risk Management Plan	30 days after task order award
Monthly Status Reports	Tuesday's beginning the second Tuesday of the month after task order award

Deliverable	Due Date (No Later Than)
EVM Reports (to be included with the Monthly Status Reports)	Tuesdays beginning the second Tuesday of the month after task order award
Meeting Minutes (e.g., Post Award Kick-Off Meeting and Status Meetings)	7 days after meeting

4.1.7 Task 2: Re-Engineering, Migration, Integration, and Implementation Services

The Contractor shall perform the following activities under this task order on a Labor-Hour basis.

The Contractor shall perform re-engineering, migration, integration, and implementation of ADAMS applications, interfaces, and business processes from IBM's FileNet Panagon Content Services platform (ADAMS) to IBM's FileNet P8 platform.

> Migration is defined as the successful transfer of one or more ADAMS application or interface, and/or business processes from its current application platform, CS (source system), to P8 (target system).
>
> Re-engineering is defined as taking existing legacy software that has become too expensive to maintain or whose system architecture or implementation are obsolete, and redeveloping it using current software and/or hardware technology. This allows a re-engineered application to take advantage and leverage the target platform's features and functions.

The Contractor shall provide re-engineering, migration, integration, and implementation services for any of ADAMS' integrated applications, interfaces, and business processes that need to be migrated to the P8 platform (see Section C.6, Integrated Applications and interfaces Dependant on ADAMS). The Contractor shall use the existing NRC applications and interfaces as templates to design and re-engineer replacements. This includes rebuilding any integrated applications and interfaces to meet requirements or creating an interface from the application to the P8 platform. The migration and re-engineering of the applications, interfaces, and business processes shall be performed in phases based on their criticality, availability, usage, etc.

The Contractor shall develop a Migration Schedule. The Contractor shall conduct the appropriate testing of the applications, interfaces, and business processes to ensure they will successfully execute on the P8 platform.

1. NRC Enterprise Architecture (EA) Standards

The Contractor shall ensure the IBM FileNet P8 platform suite of products and any non-IBM third party ECM software procured (by the NRC, not the Contractor) and provided to the Contractor under the task order shall execute in an environment containing the following technology elements and products currently implemented at NRC. As the NRC EA landscape evolves, the Contractor shall ensure the IBM FileNet P8 platform suite of products and any non-IBM third party ECM software executes in that EA.

NRC's current technology elements and products are evolving and currently include:

a) **Standard Desktop Hardware Configuration** - The current standard NRC desktop workstations are the Dell OptiPlex GX520, GX570, and 755 (PC-compatible, x8086 family, equipped with an Intel Pentium processor) running Windows XP Professional, SP2.

b) **Standard Desktop OS/Software Configuration** - The current standard NRC desktop OS and software configuration is setup with Windows XP Professional, SP2, Microsoft Office Pro 2003, Microsoft Office Outlook 2007, Internet Explorer (IE) V6, Adobe Acrobat Reader V9, Microsoft Visio 2003 Viewer and AutoCAD Design Review. *Note: A new version of IE will be implemented.*

c) **Laptop Hardware Configuration** - The current laptop models are the Dell Latitude E4300 and E6400 and a variety of other PC-compatible platforms.

d) **Laptop OS/Software Configuration** - Generally, the configuration of laptop computers follows closely those of the Standard Desktop Configuration.

e) **Web Server Hardware Configuration** - The current standard NRC web server runs on a Dell PowerEdge 2850 or an HP Proliant DL380/DL580 (equipped with Intel Pentium or Xeon processors) running with Windows Server 2003 Standard Edition, SP2. The NRC also utilizes the Sun hardware (v210, v240, v440) for its development, testing and production environments for some web servers. *Note: The models vary – predominantly HP Proliants.*

f) **Web Server OS/Software Configuration** – The current standards include Microsoft Windows Server, Internet Information Services (IIS), iPlanet Web Server Enterprise Edition, Sun ONE Web Server , Apache HTTP Server, and Oracle HTTP Server. The NRC will continue to implement web server technologies to provide efficient and stable publicly available documents. The NRC will continue to expand existing agreements with its Web-caching Contractor to duplicate the public document collection to remote sites.

g) **Application Server Hardware Configuration** - The current standard NRC application servers run on a Dell PowerEdge 2850/2950/6850 or a HP Proliant DL380/DL580 (equipped with Intel Pentium or Xeon processors) running Windows Server 2003 Standard Edition, SP2. *Note: The models actually vary quite a bit – predominantly HP Proliants.*

h) **Application Server OS/Software Configuration** - The NRC will continue to implement and integrate application server technologies like BEA WebLogic, Microsoft .Net and Oracle Application Server to provide efficient workflow infrastructure. The NRC uses a combination of Windows 2003 and 2008 server O/S in both 32-bit and 64-bit versions.

i) **Database Server Hardware Configuration** - The current standard NRC database servers run on a Dell PowerEdge 2850/2950/6850 or a HP Proliant DL380/DL580 (equipped with Intel Pentium or Xeon processors) running Windows Server 2003/2008 Standard/Enterprise Edition. *Note: The models vary quite a bit – predominantly HP Proliants.*

j) **Database Server OS/Software Configuration** - The NRC predominantly uses Microsoft SQL and Sybase database technologies. The NRC uses a combination of Windows 2003 and 2008 server O/S in both 32-bit and 64-bit versions.

k) **Storage Configuration (SAN and NAS Server)** - The NRC predominantly uses XIOTECH Magnitude 3000 storage management system, and Hitachi Data Systems Thunder modular storage system.

Note - Microsoft Office 2007 is currently targeted for FY 2010 (October 2009 – September 2010). Windows 7 is targeted for FY 2011 (October 2010 – September 2011).

Deliverables under Task 2 include:

Deliverable	Due Date (No Later Than)
Migration Schedule	60 days after task order award
Complete Migration of applications	No later than 24 months after contract award

4.2 Task 3: Synchronization of ADAMS Main Libraries

The Contractor shall perform the following activities under this task order on a Time and Materials (T&M) basis.

The Contractor shall support existing Synchronization services. The Contractor shall migrate (transfer) any remaining content from the existing Content Services repositories to the IBM FileNet P8 platform using the NRC supplied ADAMS Migration Plan as a guide (See Section J). The Contractor shall synchronize Folders, Official Agency Records, 'Other' Documents (e.g., Document Profiles, Document Security, Document Packages, etc.), Packages (an NRC construct similar in nature to a FileNet "Compound Document"), Custom Value Lists, Records Declarations, etc. between the current CS platform and the IBM FileNet P8 platform.

Deliverables under Task 3 include:

Deliverable	Due Date (No Later Than)
Synchronization Support Plan	30 days after task order award
Synchronized data	30 days after task order award until all CS systems have been decommissioned

4.3 Task 4: Operations and Maintenance (O&M) of NRC's IBM FileNet Content Services, P8 Suite of Products, ADAMS, and ADAMS Dependent Applications Listed in Table 2 of the IDIQ SOW

The Contractor shall perform the following activities under this task order on a Labor-Hour basis.

The Contractor shall provide operations and maintenance services for the Content Services OS (while it remains operational during the migration effort) and the P8 OS, and all associated applications.

The Contractor shall provide operations and maintenance services for the suite of IBM FileNet P8 products licensed at NRC including the following:

1. Content Federation Services for Content Services Server
2. Content Integrator
3. Records Crawler Server
4. E-Mail Manager Server

5. MS SharePoint Connector – Document Library
6. MS SharePoint Connector – Web Part Concurrent
7. P8 Toolkit
8. Records Manager
9. Content Collector
10. FileNet Workplace XT
11. Websphere Applications
12. Rendition Services
13. Business Process Management (BPM)
14. Business Process Framework
15. Omni Find (IBM)
16. Microsoft Office extension

The Contractor shall develop and maintain operational procedures as the components and business processes are enhanced and expended, and produce activity logs to document operations and maintenance.

The Contractor shall develop and maintain an Operations and Support Plan to include: how support will be provided, system contact personnel, defect reporting and enhancement request strategy, Service Level Agreements (SLA's), defect prioritization and resolution time periods, defect escalation criteria, how to deliver fixes into production outside the scope of an official release.

Required activities for O&M include:

a) Operating and monitoring individual components of the system.

b) Developing and maintaining operational procedures as the components and business processes are enhanced, and produce activity logs to document operations and maintenance.

c) Performing the backup and recovery strategy per OIS standard and provide an effective risk mitigation strategy for system components both during migration and in production.

d) Installing and configuring software on servers.

e) Monitoring, planning for, and updating the necessary components with vendor- issued software patches and upgrades as they become available.

f) Ensuring the integrity of the system components as they are integrated with new applications or as these applications are modified over time.

g) Monitoring, tracking, and resolving P8 end user inquiries and issues

h) Testing - The Contractor shall ensure that software products procured (by the NRC, not the Contractor) and licensed by NRC successfully execute in NRC's enterprise. The Contractor shall develop comprehensive software testing standards and plans for conducting software testing and validation. The Contractor shall develop and maintain a suite of test plans, procedures, and schedules for new deployments and upgrades of all IBM's FileNet P8 suite of products and any non-IBM third party software products. All Contractor testing shall be conducted at NRC headquarters in Rockville, MD.

i) Implementation - It is NRC's intent to employ a phased and secure approach to the implementation of IBM's FileNet P8 suite of software products and any non-IBM third party software products procured (by the NRC, not the Contractor). The software shall operate in parallel with the current ADAMS system for a period of time necessary to ensure that all users, catalogues, reports, content, business processes, and applications and interfaces are migrated to the P8 platform. The Contractor shall ensure that minimal business disruption occurs during the transition processes.

j) Training - The Contractor shall develop and maintain a Training Plan for select IBM FileNet P8 products licensed at NRC, new business processes developed under this task order, and any non-IBM third party ECM software products procured (by the NRC, not the Contractor) during the period of performance of this task order.

k) Help Desk – the Contractor shall provide 'Tier 2' level support for the IBM FileNet P8 suite of products, the P8 version of ADAMS, and new business processes developed under the task order for an estimated 5,000 users. The 'Tier 2' level support shall include providing in-depth technical support by analyzing and resolving user requests for the IBM FileNet P8 suite of products. The Contractor 'Tier 2' support staff shall work closely with the existing NRC ADAMS Help Desk to address user concerns. It is estimated that Contractor 'Tier 2' support shall be needed only for the three base years of the task order after which time the NRC ADAMS Help Desk will have gained the required technical knowledge, skills, and ability to resolve P8 user requests on their own.

Deliverables under Task 4 include:

Deliverable	Due Date (Calendar Days)
Operations and Support Plan	Specify in terms of number of days after completion of a certain task, or within a specified number of days after task order award
Test Plans (for new deployments and upgrades of all IBM's FileNet P8 suite of products and any non-IBM third party software)	Specify in terms of number of days after completion of a certain task, or within a specified number of days after task order award
Training Plan (for select IBM FileNet P8 products licensed at NRC, new business processes developed under the contract, and any non-IBM third party ECM software).	Specify in terms of number of days after completion of a certain task, or within a specified number of days after task order award

4.4 Task 5: Security

The NRC intends to use another Contractor ("NRC's security Contractor") to serve as the primary developer of deliverables needed for the Security Certification and Accreditation of ADAMS and related systems.

The Contractor shall perform the following activities under this task order on a time and materials (T&M) basis. The Contractor shall work with the Project Officer to provide them the information they need to provide to the security Contractor so that they can develop the deliverables required for the Security Certification and Accreditation of ADAMS and related systems.

4.4.1 Basic Task Order IT Security Requirements

For unclassified information used for the effort, the Contractor shall coordinate with the NRC Project Officer to provide them the information they need to develop an information security categorization document indicating the sensitivity of the information processed as part of this task order if the information security categorization was not provided in the PWS. The determination shall be made using NIST SP 800-60 and must be approved by the Computer Security Office (CSO). The NRC Contracting Officer and Project Officer shall be notified immediately before the Contractor begins to process information at a higher sensitivity level.

The Contractor shall immediately notify the Contracting Officer and the NRC Project Officer if the Contractor begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the Contractor shall immediately notify the Contracting Officer and Project Officer if the Contractor begins to process *information at a more restrictive classification level.

All work under this task order shall comply with the latest versions of the following guidance and standards to include NRC Management Directive 12.5 Automated Information Security Program, and National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS), and Committee on National Security Systems (CNSS) policy, policy, directives, instructions, and guidance. This information is available at the following links:

NRC Policies, Procedures and Standards (Computer Security Office (CSO) internal website):
http://www.internal.nrc.gov/CSO/policies.html

All NRC Management Directives (public website):
http://www.nrc.gov/reading-rm/doc-collections/management-directives/

NIST SP and FIPS documentation is located at:
http://csrc.nist.gov/

CNSS documents are located at:
http://www.cnss.gov/

When e-mail is used, the Contractor shall only use NRC provided e-mail accounts to send and receive sensitive information (information that is not releasable to the public) or mechanisms to protect the information during transmission to NRC that have been approved by NRC CSO.

All Contractor personnel must sign the NRC Agency-wide Rules of Behavior for Secure Computer Use prior to being granted access to NRC computing resources.

The Contractor shall adhere to NRC policies, including:

- Management Directive 12.5, Automated Information Security Program
- Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
- Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
- Computer Security Information Protection Policy
- Remote Access Policy
- Use of Commercial Wireless Devices, Services and Technologies Policy
- Laptop Security Policy
- Computer Security Incident Response Policy

The Contractor shall not use personal devices to process and store NRC sensitive information.

All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been previously certified and accredited by NRC for processing information at the sensitivity level of the information being processed.

4.4.2 Purging of NRC Data from Contractor Systems

The Contractor shall ensure that the NRC data processed during the performance of this task order is purged from all data storage components of the Contractor's computer facility, and the Contractor will shall not retain any NRC data after 30 days of completion of the period of performance for this task order.

The Contractor shall notify the Project Officer in writing within 24 hours after determining that one or more Contractor personnel no longer require access to an NRC system Contractor. Such notification shall include the name(s) of Contractor personnel and the NRC system(s) for which they no longer require access.

Upon task order completion, the Contractor shall provide a status list to the Project Officer of all Contractor personnel that are still NRC system users and shall note if any of those users still require access to the system(s) to perform work on other contracts or orders that are in place and active at that time.

4.4.3 Access Controls

Any Contractor system being used to process NRC data shall be able to define and enforce access privileges for individual users. The discretionary access controls mechanisms shall be configurable to protect objects (e.g., files, folders) from unauthorized access.

The Contractor system being used to process NRC data shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

Contractor personnel shall only use NRC approved methods to send and receive information considered sensitive or classified. Specifically,

- **Classified Information -** All NRC Classified data being transmitted over a network shall use NSA approved encryption and adhere to guidance in NRC Management Directive (MD) 12.2 NRC Classified Information Security Program, MD 12.5 NRC Automated Information Security Program and Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing.

- **SGI Information –** All SGI being transmitted over a network shall adhere to guidance in MD 12.7 NRC Safeguards Information Security Program and MD 12.5 NRC Automated Information Security Program. SGI processing shall be only within facilities, computers, and spaces that have been specifically approved for SGI processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The 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.

The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.

Separation of duties for Contractor systems used to process NRC information must be enforced by the system through assigned access authorizations.

The mechanisms within the Contractor system or application that enforces access control and other security features shall be continuously protected against tampering and/or unauthorized changes.

4.4.4 Configuration Standards

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: http://www.internal.nrc.gov/CSO/standards.html .

4.4.5 Media Handling

All media used by the Contractor to store or process NRC information shall be controlled in accordance to the sensitivity level.

The Contractor shall not perform sanitization or destruction of media approved for processing NRC information designated as SGI or Classified. The Contractor must provide the media to NRC for destruction.

4.4.6 Vulnerability Management

The Contractor must adhere to NRC patch management processes for all systems used to process NRC information. Patch Management reports will made available to the Contractor upon written request to the Project Officer for following security categorizations and reporting timeframes:

- 5 calendar days after being requested for a high sensitivity system
- 10 calendar days after being requested for a moderate sensitivity system
- 15 calendar days after being requested for a low sensitivity system

For any Contractor system used to process NRC information, the Contractor must ensure that information loaded into the system is scanned for viruses prior to posting; servers are scanned for viruses, adware, and spyware on a regular basis; and virus signatures are updated at the following frequency:

- 1 calendar day for a high sensitivity system
- 3 calendar days for a moderate sensitivity system
- 7 calendar days for a low sensitivity system

4.4.7 Application Security Requirements

The Contractor shall correct errors in Contractor developed software and applicable documentation that are not commercial off-the-shelf which are brought to the attention of the Contractor in writing by the Contracting Officer, Project Officer or the or the Contractor's personnel. The Contractor shall adhere to the guidance outlined in NIST SP 800-53, FIPS 200 and NRC guidance for the identification and documentation of minimum security controls.

All development and testing of the systems shall be protected at their assigned system sensitivity level and shall be performed on a network separate and isolated from the NRC operational network.

All system computers must be properly configured and hardened according to NRC policies, guidance, and standards and comply with all NRC security policies and procedures as commensurate with the system security categorization.

4.4.8 Access Controls

The Contractor shall not hardcode any passwords into the software unless the password only appears on the server side (e.g. using server-side technology such as ASP, PHP, or JSP).

The Contractor shall ensure that the software does not contain undocumented functions and undocumented methods for gaining access to the software or to the computer system on which it is installed. This includes master access keys, back doors, and trapdoors.

4.4.9 Cryptography

The Contractor shall validate cryptographic modules provided as part of the system under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 and must be operated in FIPS mode. The Contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module to the Project Officer that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

4.4.10 Control of Hardware and Software

The Contractor shall demonstrate to the Project Officer that all hardware and software meet security requirements prior to being placed into the NRC production environment.

The Contractor shall ensure that the development environment is separated from the operational environment using NRC CSO approved controls.

The Contractor shall only use licensed software and in-house developed authorized software (including NRC and Contractor developed) on the system and for processing NRC information. Public domain, shareware, or freeware may only be installed by the Contractor after prior written approval is obtained from the Project Officer.

The Contractor shall provide proof of valid software licensing upon request of the Contracting Officer or the Project Officer.

4.4.11 Information Security Training and Awareness Training

The Contractor shall ensure that its personnel (including subcontractors), in performance of the task order, receive Information Technology (IT) security training in their role at the Contractor's expense. The Contractor must provide the NRC written certification that training is complete, along with the title of the course and dates of training as a prerequisite to start of work on the task order.

The IT security role and associated type of training course and periodicity required to be completed are as follows:

Role	Type of Training	Required Frequency of Training
Auditor	Vendor specific operating system and application security training, database security training	Prior to appointment and then every three years
IT Functional Manager	Vendor specific operating system and application security training, database security training	Prior to appointment and then every two years Additional system specific training upon a major system update/change
System	Vendor specific operating	Prior to appointment and then

Role	Type of Training	Required Frequency of Training
Administrator	system and application security training	every year: • Training in operating system security in the area of responsibility occurs every 2 years • Training in application security in the area of responsibility occurs every 2 years
Information Systems Security Officer	ISSO role specific training (not awareness) provided by a government agency or by a vendor such as SANS Vendor specific operating system and application security training	Prior to appointment and then every year: • Training in the ISSO role occurs every 3 years • Training in operating system security in the area of responsibility occurs every 3 years • Training in application security in the area of responsibility occurs every 3 years
Database Administrator	Vendor specific database security training	Prior to appointment and then every 2 years: • Training in database security in the area of responsibility occurs every 2 years
Network Administrator	Network administrator role specific training (not awareness) provided by a government agency or by a vendor such as SANS Network specific security training	Prior to appointment and then every year: • Training in the Network administrator role occurs every 3 years • Training in network security in the area of responsibility occurs every year where network administrator role training does not occur
IT Managers	Vendor specific operating system and application security training, database security training.	Prior to appointment and then every two years Additional system specific training upon a major system update/change
IT System	Vendor specific operating	Prior to appointment and then

Role	Type of Training	Required Frequency of Training
Developer	system and application security training, database security training	every year • Training with system-specific training (ISS LoB or commercial) upon assuming the role, to become biannual with NRC provided training every other year.

The Contractor must ensure that required refresher training is accomplished in accordance with the required frequency specifically associated with the IT security role.

4.4.12 Auditing

The system (ADAMS and ADAMS integrated applications and interfaces described in Table 2 of the IDIQ SOW) shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

The system (ADAMS and ADAMS integrated applications and interfaces described in Table 2 of the IDIQ SOW) shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators or system security officers and other security relevant events. The system shall be able to audit any override of security controls.

The Contractor shall ensure auditing is implemented on the following:

- Operating System
- Application
- Web Server
- Web Services
- Network Devices
- Database
- Wireless

The Contractor shall perform audit log reviews daily using automated analysis tools.

The Contractor must log at least the following events on systems that process NRC information:

a. Audit all failures
b. Successful logon attempt
c. Failure of logon attempt
d. Permission Changes
e. Unsuccessful File Access
f. Creating users & objects
g. Deletion & modification of system files
h. Registry Key/Kernel changes
i. Startup & shutdown
j. Authentication

k. Authorization/permission granting
l. Actions by trusted users
m. Process invocation
n. Controlled access to data by individually authenticated user
o. Unsuccessful data access attempt
p. Data deletion
q. Data transfer
r. Application configuration change
s. Application of confidentiality or integrity labels to data
t. Override or modification of data labels or markings
u. Output to removable media
v. Output to a printer

4.4.13 Certification and Accreditation

4.4.13.1 Security Risk Assessment

The Contractor shall coordinate with the NRC [Project Officer in performing Risk Assessment activities according to NRC policy, standards, and guidance. The Contractor shall coordinate with the Project Officer to provide them the information they need to perform Risk Assessment activities that include analyzing how the architecture implements the NRC documented security policy for the system, assessing how management, operational, and technical security control features are planned or implemented and how the system interconnects to other systems or networks while maintaining security.

4.4.13.2 System Security Plan

The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to develop the system security plan (SSP) according to NRC policy, standards, and guidance to define the implementation of IT security controls necessary to meet both the functional assurance and security requirements. The Contractor will coordinate with the Project Officer to provide them the information they need to ensure that all controls required to be implemented are documented in the SSP.

4.4.13.3 Assessment Procedures – Security Test & Evaluation

The Contractor shall coordinate with the Project Officer to provide them the information they need to follow NRC policy, standards, and guidance for execution of the test procedures. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to NRC. The Contractor shall coordinate with the Project Officer to provide them the information they need to include verification and validation to ensure that appropriate corrective action was taken on identified security weaknesses.

The Contractor shall coordinate with the Project Officer to provide them the information they need to develop perform ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan, execution ST&E test cases and documentation of test results. The Contractor shall coordinate with the Project Officer to provide them the information they need to prepare the Plan of Action and Milestones (POA&M) based on the ST&E results.

4.4.13.4 Plan of Action and Milestones (POA&M) Maintenance & Reporting

The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to provide a determination on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risked-based decisions. The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to develop and implement solutions that provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items.

The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to develop perform verification of IT security weaknesses to ensure that all weaknesses identified through third party (e.g., OIG) audits are included in the POA&Ms that the quarterly reporting to OMB is accurate, and the reasons for any exceptions or risked-based decisions are reasonable and clearly documented. This verification process will be done in conjunction with the continuous monitoring activities.

4.4.13.5 Certification & Accreditation Documentation

The Contractor shall coordinate with the Project Officer to provide them the information they need to create, update maintain all Certification and Accreditation (C&A) documentation in accordance with the following NRC Certification and Accreditation procedures and guidance:

- C&A Non-SGI Unclassified Systems
- C&A SGI Unclassified Systems
- C&A Classified Systems

Contractor must coordinate with the Project Officer to provide them the information they need to develop contingency plan and ensure annual contingency testing is completed within one year of previous test and provide an updated security plan and test report according to NRC's policy and procedure.

Contractor must coordinate with the Project Officer to provide them the information they need to conduct annual security control testing according to NRC's policy and procedure and update POA&M, SSP, etc. to reflect any findings or changes to management, operational and technical controls.

The Contractor shall coordinate with the Project Officer to provide them the information they need to perform, document and report to NRC management the results of continuous monitoring activities which include to the following: assessment of selected security controls, configuration management, security impact analysis on changes, C&A documentation updates.

The Contractor shall coordinate with the Project Officer to provide them the information they need to meet the Continuous Monitoring requirements identified in NIST Special Publication 800-37.

The Contractor shall coordinate with the NRC Project Officer to provide them the information they need to develop the FISMA/ National Institute of Standards and Technology (NIST) required C&A documentation. The system (ADAMS and ADAMS integrated applications and interfaces described in Table 2 of the IDIQ SOW) shall meet content security requirements as well as U.S. Department of Defense (DoD) 5015.2-STD Electronic Recordkeeping System compliance requirements.

5.0 Instructions for Deliverables

Each deliverable shall first be submitted in draft to the Project Officer for NRC review. NRC shall have 10 days to review each draft deliverable and respond with comments or approval. If the Project Officer does not provide written comments to the Contractor at the end of 10 days, the Contractor shall assume the deliverable has been approved.

If revisions are required, the Contractor has 5 days to complete the revisions and submit the revised draft deliverable to the Project Officer. For each deliverable (draft and final), the Contractor shall provide one (1) electronic version of the deliverable via e-mail to the NRC Project Officer, unless otherwise indicated.

All deliverables and supporting documentation gathered or developed under this task order may not be stored on any device or piece of equipment that has not been approved in writing by the Project Officer.

All deliverables shall be:

a. Free of formatting and spelling errors, be clearly written, and have no incomplete sections.

b. Submitted in electronic format and shall be free of computer viruses. If a virus is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus or defect.

c. "Plain English" written in language that can be understood by a non-technical layperson. Statistical and other technical terms used in the deliverable shall be defined in a glossary.

d. Formatted in Microsoft Word (version 2003 or later). The Project Plan must be formatted in Microsoft Project (version 2003 or later).

e. Timely, thorough, and accurate. Accompanied by a cover letter from the Contractor on company letterhead. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.

6.0 Period of Performance

The period of performance for this task order is 1 year from the date of award. For proposal preparation purposes, assume that the task order will start on October 1, 2010.

7.0 Government Provided Space

The place of performance is at the government site, NRC's King of Prussia Facility, King of Prussia, PA and NRC Headquarters, Rockville, MD.

The NRC will provide a fully functional office environment for contractor personnel within NRC's facilities located in Region I and NRC Headquarters. Within this office space, the NRC will provide desktop workstations with all software needed to perform the work specified under this task order. The NRC will also provide two telephones and access to computer printing and photo copying equipment.

NRC Headquarters

One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

or

Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

8.0 Travel

The contractor will be reimbursed in accordance with FAR Subpart 31.205-46 for reasonable domestic travel costs incurred during the performance of this task order for the purpose of providing support under this task order. All Contractor travel shall be approved in writing by the Project Officer prior to the Contractor incurring travel costs. Performance under this task order may require travel to NRC's four regional offices located in:

U.S. NRC Region I
475 Allendale Road
King of Prussia, PA 19406-1415

U.S. NRC Region II
Sam Nunn Atlanta Federal Center, 23
T85 61 Forsyth Street, SW
Atlanta, GA 30303-8931

U.S. NRC Region III
2443 Warrenville Road
Suite 210
Lisle, Illinois 60532-4352

U.S. NRC Region IV
Texas Health Resources Tower
612 E. Lamar Blvd., Suite 400
Arlington, TX 76011-4125

9.0 Meetings

All meetings shall be held at NRC Headquarters in Rockville, MD. When possible, meetings will be conducted via teleconference or videoconference.

9.1 Project Kick-Off (Post-Award) Meeting

Within seven days of task order award, the Contractor shall convene a project kick-off meeting with the Project Officer, the NRC primary stakeholders, and Contractor personnel working on this task order. Activities for this meeting shall include

- A confirmation of the Project's objectives
- A submission and discussion of a draft high level Baseline Project Plan and Project Approach Summary
- An identification of key points of contact
- A discussion of project related administrative and logistical processes.

9.2 Weekly Meetings

The Contractor shall meet with the Project Officer on a weekly basis for the purpose of clearly articulating the project's status and to address any questions or concerns the NRC might have.

9.3 Ad-Hoc Meetings

The Contractor shall be available to attend Ad-Hoc meetings requested by the Project Officer. The Contractor will be given ***24 hours*** written notice before an Ad-Hoc Meeting will be held.

10.0 Weekly Progress Reports

The Contractor will provide the Project Officer with Weekly progress reports that address the following:

- Status (on schedule, behind schedule)
- Budget (amount of contract dollars used during the last week for labor-hour tasks only
- Completed activities (includes list of deliverables submitted to the Project Officer for review)
- Ongoing Activities
- Planned activities.
- Identified Issues and Risks

The weekly progress reports will be due to the Project Officer by 5:00 pm Eastern Time each Monday. If Monday is a federal holiday, the report will be due by 5:00pm Eastern Time on the next business day.

A.1 2052.215-70 KEY PERSONNEL (JAN 1993)

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

James Baldwin, Project Manager

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

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

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

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