

ADDITIONAL TASK ORDER TERMS AND CONDITIONS

Table of Contents

A.1 PROJECT TITLE 2
A.2 BRIEF DESCRIPTION OF WORK (MAR 1987) 2
A.3 CONTRACT TYPE 2
A.4 CONSIDERATION AND OBLIGATION--DELIVERY ORDERS (JUN 1988) 2
A.5 OPTION PERIODS - TASK ORDER/DELIVERY ORDER UNDER A GSA FEDERAL
SUPPLY SCHEDULE CONTRACT (MARCH 2007) 3
A.6 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL
II ACCESS APPROVAL (JUL 2007) 3
A.7 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY (JANUARY 2001) 5
A.8 SEAT BELTS 6
A.9 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS 6
A.10 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL 7
A.11 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY
(IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002) 7
A.12 COMPLIANCE WITH US IMMIGRATION LAWS AND REGULATIONS 7
A.13 SAFETY OF ON-SITE CONTRACTOR PERSONNEL 8
A.14 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2003) 8
A.15 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR
EMPLOYEES (JULY 2006) 9
A.16 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS
(JUNE 2006) 9
A.17 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR
FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS
INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (DEC 2008)9
A.18 2052.204-70 SECURITY (MAR 2004) 10
A.19 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO
NRC FACILITIES (MAR 2006) 12
A.20 2052.209-72 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST (JAN
1993) 12
A.21 2052.211-70 PREPARATION OF TECHNICAL REPORTS (JAN 1993) 15
A.22 2052.211-71 TECHNICAL PROGRESS REPORT (JAN 1993) 15
A.23 2052.211-72 FINANCIAL STATUS REPORT (OCT 1999) 15
A.24 2052.215-70 KEY PERSONNEL (JAN 1993) 17
A.25 PROJECT OFFICER AUTHORITY ALTERNATE 2 (FEBRUARY 2004) 17
A.26 2052.215-78 TRAVEL APPROVALS AND REIMBURSEMENT -ALTERNATE 1 (OCT
1999) 18
A.27 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 18
A.28 PROJECT SUPPORT CONTRACTORS 18
A.29 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999) 19
A.30 LIST OF ATTACHMENTS 20

A.1 PROJECT TITLE

The title of this project is as follows:
 Operations and Maintenance for the Digital Data Management System.

A.2 BRIEF DESCRIPTION OF WORK (MAR 1987)

The Contractor shall provide all necessary personnel and materials required in support the Operations and maintenance support for the DDMS installations at the Rockville hearing room and the Las Vegas hearing facility. The contractor shall also support the application installations in the Consolidated Test Facility (CTF), the Test and Acceptance Environment (TAE), and/or the contractor development lab. In addition the contractor shall provide Day-to-day hearing support for hearings held at the Rockville Hearing room, the Las Vegas Hearing Facility, and remote locations or other hearing sites throughout the United States and its territories.

A.3 CONTRACT TYPE

This contract will contain firm fixed price tasks and time and materials tasks. See attachment 1, entitled: Price Schedule for details.

Task Number	Task Title	Contract Type
Task 1	Operations and Maintenance (General, daily and weekly tasks):	Firm Fixed Price
Task 1a	Operations and Maintenance "As needed tasks"	Time and Materials
Task 2	IT Security Related Activities	Time and Materials
Task 3	Hearing / Meeting Support	Time and Materials
Task 4	Application Enhancements, Development and Test Environment	Time and Materials
Task 5	Training	Firm Fixed Price per training session
Optional Task 6a	Technology Refresh of Rockville Data Processing sub-system	Time and Materials
Optional Task 6b	Technology Refresh of Las Vegas Data Processing sub-system	Time and Materials
Optional Task 6c	Technology Refresh of Rockville Audio Visual Sub-System	Time and Materials
Optional Task 6d	Technology Refresh of Las Vegas Audio Visual Sub-System	Time and Materials
Optional task 7	Transition Task	Firm Fixed Price

A.4 CONSIDERATION AND OBLIGATION--DELIVERY ORDERS (JUN 1988)

(a) The total estimated amount of this contract (ceiling) for the products/services ordered, delivered, and accepted under this contract is 1,456,535.98. The Contracting Officer may unilaterally increase this amount as necessary for orders to be placed with the contractor during the contract period provided such orders are within any maximum ordering limitation prescribed under this contract.

(b) The amount presently obligated with respect to this contract is 900,000. The Contracting Officer may issue orders for work up to the amount presently obligated. This obligated amount may be unilaterally increased from time to time by the Contracting Officer by written modification to this contract. The obligated amount shall, at no time, exceed the 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.5 OPTION PERIODS - TASK ORDER/DELIVERY ORDER UNDER A GSA FEDERAL SUPPLY SCHEDULE CONTRACT (MARCH 2007)

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

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

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

A.6 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (JUL 2007)

The proposer/Contractor must identify all individuals and propose the level of Information Technology (IT) approval for each, using the following guidance. The NRC sponsoring office shall make the final determination of the level, if any, of IT approval required for all individuals working under this contract. The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating IT access approvals for individuals performing work under this contract.

The Contractor shall conduct a preliminary security interview or review for each IT level I or II access approval Contractor applicant and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of IT security access for which the candidate has been proposed. The Contractor will pre-screen its applicants for the following:

(a) felony arrest in the last seven years; (b) alcohol related arrest within the last five years; (c) record of any military courts-martial convictions in the past ten years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven years; (e) delinquency on any federal debts or bankruptcy in the last seven years.

The Contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the applicant verify the pre-screening record or review, sign and date it. Two copies of the signed Contractor's pre-screening record or review will be supplied to FSB/DFS with the Contractor employee's completed building access application package.

The Contractor shall further ensure that its employees, any subcontractor employees and consultants complete all IT access security applications required by this clause within ten business days of notification by FSB/DFS of initiation of the application process. Timely receipt of properly completed records of the pre-screening record and IT access security applications (submitted for candidates that have a reasonable probability of obtaining the level of security assurance necessary for access to NRC's facilities) is a contract requirement. Failure of the Contractor to comply with this contract administration requirement may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of cancellation or termination, the NRC may select another firm for contract award.

SECURITY REQUIREMENTS FOR IT LEVEL I

Performance under this contract will involve prime Contractor personnel, subcontractors or others who perform services requiring direct access to or operate agency sensitive information technology systems or data (IT Level I). The IT Level I involves responsibility for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning, and design of a computer system, including hardware and software; or the capability to access a computer system during its operation or maintenance in such a way that could cause or that has a relatively high risk of causing grave damage; or the capability to realize a significant personal gain from computer access.

A Contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary IT access may be approved based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved based on a favorable review or adjudication. However, temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a reinvestigation every ten years.

The Contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 85P (Questionnaire for Public Trust Positions), two copies of the Contractor's signed pre-screening record and two FD 258 fingerprint charts, through the PO to FSB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The Contractor shall assure that all forms are accurate, complete, and legible. Based on FSB/DFS review of the Contractor applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility.

In accordance with NRCAR 2052.204 70 "Security," IT Level I Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments) and SF- 85P which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others (e.g., bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

SECURITY REQUIREMENTS FOR IT LEVEL II

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

The IT Level II involves responsibility for the planning, design, operation, or maintenance of a computer system and all other computer or IT positions.

A Contractor employee shall not have access to sensitive information technology systems or data until he/she is approved by FSB/DFS. Temporary access may be approved based on a favorable review of their security forms and checks. Final IT access may be approved based on a favorable adjudication. However, temporary access authorization approval will be revoked and the employee may subsequently be denied IT access in the event the employee's investigation cannot be favorably adjudicated. Such an employee will not be authorized to work under any NRC contract requiring IT access without the approval of FSB/DFS. Where temporary access authorization has been revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. When an individual receives final IT access, the individual will be subject to a review or reinvestigation every ten years.

The Contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 85P (Questionnaire for Public Trust Positions), two copies of the Contractor's signed pre-screening record and two FD 258 fingerprint charts, through the PO to FSB/DFS for review and favorable adjudication, prior to the individual performing work under this contract. The Contractor shall assure that all forms are accurate, complete, and legible. Based on FSB/DFS review of the Contractor applicant's security forms and/or the receipt of adverse information by NRC, the individual may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made of his/her eligibility.

In accordance with NRCAR 2052.204 70 "Security," IT Level II Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments), SF- 85P, and Contractor's record of the pre-screening which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others (e.g. bidders) who have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

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

A.7 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY (JANUARY 2001)

(a) The NRC will provide the contractor with the following items for use under this contract:

1. See attachment II - Entitled: Inventory

(b) The above listed equipment/property is hereby transferred from the government .

(c) Only the equipment/property listed above in the quantities shown will be provided by the Government. The contractor shall be responsible and accountable for all Government property 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 to the NRC Contracting Officer (CO) and the NRC Division of Facilities and Security, Physical Security Branch of all cases of loss, damage, or destruction of Government property in its possession or control not later than 24 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 Division of Facilities and Security, Physical Security Branch.

(d) All other equipment/property required in performance of the contract shall be furnished by the Contractor.

A.8 SEAT BELTS

Contractors, subcontractors, and grantees, are encouraged to adopt and enforce on-the-job seat belt policies and programs for their employees when operating company-owned, rented, or personally owned vehicles.

A.9 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS

Annual and final evaluations of contractor performance under this contract will be prepared in accordance with FAR 42.15, "Contractor Performance Information," normally at the time the contractor is notified of the NRC's intent to exercise the contract option. If the multi-year contract does not have option years, then an annual evaluation will be prepared (state time for annual evaluation). Final evaluations of contractor performance will be prepared at the expiration of the contract during the contract closeout process.

The Contracting Officer will transmit the NRC Project Officer's annual and final contractor performance evaluations to the contractor's Project Manager, unless otherwise instructed by the contractor. The contractor will be permitted thirty days to review the document. The contractor may concur without comment, submit additional information, or request a meeting to discuss the performance evaluation. The Contracting Officer may request the contractor's Project Manger to attend a meeting to discuss the performance evaluation.

Where a contractor concurs with, or takes no exception to an annual performance evaluation, the Contracting Officer will consider such evaluation final and releasable for source selection purposes. Disagreements between the parties regarding a performance evaluation will be referred to an individual one level above the Contracting Officer, whose decision will be final.

The Contracting Officer will send a copy of the completed evaluation report, marked "For Official Use Only," to the contractor's Project Manager for their records as soon as practicable after it has been finalized. The completed evaluation report also will be used as a tool to improve communications between the NRC and the contractor and to improve contract performance.

The completed annual performance evaluation will be used to support future award decisions in accordance with FAR 42.1502(a) and 42.1503(c). During the period the information is being used to provide source selection information, the completed annual performance evaluation will be released to only two parties - the Federal government personnel performing the source selection evaluation and the contractor under evaluation if the contractor does not have a copy of the report already.

A.10 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL

a. NRC facilities may not be available due to (1) designated Federal holiday, any other day designated by Federal Statute, Executive Order, or by President's Proclamation; (2) early dismissal of NRC employees during working hours (e.g., special holidays, water emergency); or (3) occurrence of emergency conditions during nonworking hours (e.g., inclement weather).

b. When NRC facilities are unavailable, the contractor's compensation and deduction policy (date), incorporated herein by reference, shall be followed for contractor employees performing work on-site at the NRC facility. The contractor shall promptly submit any revisions to this policy to the Contracting Officer for review before they are incorporated into the contract.

c. The contractor shall not charge the NRC for work performed by on-site contractor employees who were reassigned to perform other duties off site during the time the NRC facility was closed.

d. On-site contractor staff shall be guided by the instructions given by a third party (e.g., Montgomery County personnel in situations which pose an immediate health or safety threat to employees (e.g., water emergency).

e. The contractor's Project Director shall first consult the NRC Project Officer before authorizing leave for on-site personnel in situations which do not impose an immediate safety or health threat to employees (e.g., special holidays). That same day, the contractor must then alert the Contracting Officer of the NRC Project Officer's direction. The contractor shall continue to provide sufficient personnel to perform the requirements of essential tasks as defined in the Statement of Work which already are in operation or are scheduled.

A.11 APPROPRIATE USE OF GOVERNMENT FURNISHED INFORMATION TECHNOLOGY (IT) EQUIPMENT AND/ OR IT SERVICES/ ACCESS (MARCH 2002)

As part of contract performance the NRC may provide the contractor with information technology (IT) equipment and IT services or IT access as identified in the solicitation or subsequently as identified in the contract or delivery order. Government furnished IT equipment, or IT services, or IT access may include but is not limited to computers, copiers, facsimile machines, printers, pagers, software, phones, Internet access and use, and email access and use. The contractor (including the contractor's employees, consultants and subcontractors) shall use the government furnished IT equipment, and / or IT provided services, and/ or IT access solely to perform the necessary efforts required under the contract. The contractor (including the contractor's employees, consultants and subcontractors) are prohibited from engaging or using the government IT equipment and government provided IT services or IT access for any personal use, misuse, abuses or any other unauthorized usage.

The contractor is responsible for monitoring its employees, consultants and subcontractors to ensure that government furnished IT equipment and/ or IT services, and/ or IT access are not being used for personal use, misused or abused. The government reserves the right to withdraw or suspend the use of its government furnished IT equipment, IT services and/ or IT access arising from contractor personal usage, or misuse or abuse; and/ or to disallow any payments associated with contractor (including the contractor's employees, consultants and subcontractors) personal usage, misuses or abuses of IT equipment, IT services and/ or IT access; and/ or to terminate for cause the contract or delivery order arising from violation of this provision.

A.12 COMPLIANCE WITH US IMMIGRATION LAWS AND REGULATIONS

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States Immigration and Naturalization (INS) laws and regulations, including employment authorization documents and visa requirements. Each alien employee of the Contractor must be lawfully admitted for permanent residence as evidenced by Alien Registration Receipt Card Form 1-151 or must present other evidence from the Immigration and Naturalization Services that employment will not affect his/her immigration status. The INS Office of Business Liaison (OBL) provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on the INS website, <http://www.ins.usdoj.gov/graphics/services/employerinfo/index.htm#obl>.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC facilities or its equipment/services, and/or take any number of contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

A.13 SAFETY OF ON-SITE CONTRACTOR PERSONNEL

Ensuring the safety of occupants of Federal buildings is a responsibility shared by the professionals implementing our security and safety programs and the persons being protected. The NRC's Office of Administration (ADM) Division of Facilities and Security (DFS) has coordinated an Occupant Emergency Plan (OEP) for NRC Headquarters buildings with local authorities. The OEP has been approved by the Montgomery County Fire and Rescue Service. It is designed to improve building occupants' chances of survival, minimize damage to property, and promptly account for building occupants when necessary.

The contractor's Project Director shall ensure that all personnel working full time on-site at NRC Headquarters read the NRC's OEP, provided electronically on the NRC Intranet at <http://www.internal.nrc.gov/ADM/OEP.pdf>. The contractor's Project Director also shall emphasize to each staff member that they are to be familiar with and guided by the OEP, as well as by instructions given by emergency response personnel in situations which pose an immediate health or safety threat to building occupants.

The NRC Project Officer shall ensure that the contractor's Project Director has communicated the requirement for on-site contractor staff to follow the guidance in the OEP. The NRC Project Officer also will assist in accounting for on-site contract persons in the event of a major emergency (e.g., explosion occurs and casualties or injuries are suspected) during which a full evacuation will be required, including the assembly and accountability of occupants. The NRC DFS will conduct drills periodically to train occupants and assess these procedures.

A.14 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2003)

NRC contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day.

Contractor employees, consultants, and subcontractors shall complete the NRC's online, "Computer Security Awareness" course on the same day that they receive access to the agency's IT equipment and/or services, as their first action using the equipment/service. For those contractor employees, consultants, and subcontractors who are already working under this contract, the on-line training must be completed in accordance with agency Network Announcements issued throughout the year 2003 within three weeks of issuance of this modification.

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the NRC

throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

The NRC reserves the right to deny or withdraw Contractor use or access to NRC IT equipment and/or services, and/or take other appropriate contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

A.15 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.16 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (JUNE 2006)

Prior to occupying any government provided space at the NRC Headquarters in Rockville, Maryland, the Contractor shall obtain written authorization to occupy specifically designated government space via the NRC Project Officer from the Chief, Space Planning and Property Management Branch, Division of Facilities and Security. Failure to obtain this prior authorization may result in one or a combination of the following remedies as deemed appropriate by the Contracting Officer.

1. Rental charge for the space occupied to be deducted from invoice amount due the Contractor
2. Removal from the space occupied
3. Contract Termination

A.17 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (DEC 2008)

NRC's Headquarters Assistant Drug Program Coordinator (ADPC) shall be responsible for implementing and managing the collecting and testing portions of the NRC Contractor Drug Testing Program. The Headquarters ADPC function is carried out by the Drug Program Manager in the Division of Facilities and Security, Office of Administration.

All sample collection, testing, and review of test results shall be conducted by the NRC "drug testing contractor." The NRC will reimburse the NRC "drug testing contractor" for these services.

All contractor employees, subcontractor employees, and consultants proposed for performance or performing under this contract shall be subject to the requirements of the clause if they meet one of the following criteria stated in the Plan: (1) individuals who require unescorted access to nuclear power plants, (2) individuals who have access to classified or safeguards information, (3) individuals who are required to carry firearms in performing security services for the NRC, (4) individuals who are required to operate government vehicles or transport passengers for the NRC, (5) individuals who are required to operate hazardous equipment at NRC facilities, or (6) individuals who admit to recent illegal drug use or those who are found through other means to be using drugs illegally. The Plan includes pre-assignment, random, reasonable suspicion, and post-accident drug testing. The due process procedures applicable to NRC employees under NRC's Drug Testing Program are not applicable to contractors, consultants, subcontractors and their employees. Rather, a contractor's employees and their subcontractors are subject to the procedures and terms of their employment agreements with their employer.

The NRC Drug Program Manager will schedule the drug testing for all contractor employees, subcontractor employees, and consultants who are subject to testing under this clause in accordance with the Plan. The NRC will reimburse the NRC "drug testing contractor" for collecting, testing, and reviewing test results. Any NRC contractor found to be using, selling, or possessing illegal drugs, or any contractor with a verified positive drug test result under this program while in a duty status will immediately be removed from working under the NRC contract. The contractor's employer will be notified of the denial or revocation of the individual's authorization to have access to information and ability to perform under the contract. The individual may not work on any NRC contract for a period of not less than one year from the date of the failed drug test and will not be considered for reinstatement unless evidence of rehabilitation, as determined by the NRC "drug testing contractor's" Medical Review Officer, is provided.

Contractor drug testing records are protected under the NRC Privacy Act Systems of Records, System 35, "Drug Testing Program Records - NRC" found at: <http://www.nrc.gov/reading-rm/foia/privacy-systems.html>

A.18 2052.204.70 SECURITY (MAR 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 sensitive unclassified information (e.g., Safeguards), 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, 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 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.19 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES
(MAR 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.20 2052.209-72 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST (JAN 1993)

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

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

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

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

(c) Work for others.

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

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

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

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

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

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

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

(d) Disclosure after award.

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

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

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

approval of the disclosed work only when the NRC has issued a task order which includes the technical area and, if site-specific, the site, or has plans to issue a task order which includes the technical area and, if site-specific, the site, or when the work violates paragraphs (c)(2), (c)(3) or (c)(4) of this section.

(e) Access to and use of information.

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

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

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

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

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

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

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

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

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

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

(i) Follow-on effort. The contractor shall be ineligible to participate in NRC contracts, subcontracts, or proposals 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.21 2052.211-70 PREPARATION OF TECHNICAL REPORTS (JAN 1993)

All technical reports required by Section C and all Technical Progress Reports required by Section F are to be prepared in accordance with the attached Management Directive 3.8, "Unclassified Contractor and Grantee Publications in the NUREG Series." Management Directive 3.8 is not applicable to any Contractor Spending Plan (CSP) and any Financial Status Report that may be included in this contract. (See List of Attachments).

A.22 2052.211-71 TECHNICAL PROGRESS REPORT (JAN 1993)

The contractor shall provide a monthly Technical Progress Report to the project officer and the contracting officer. The report is due within 15 calendar days after the end of the report period and must identify the title of the project, the contract number, appropriate financial tracking code specified by the NRC Project Officer, project manager and/or principal investigator, the contract period of performance, and the period covered by the report. Each report must include the following for each discrete task/task order:

(a) A listing of the efforts completed during the period, and milestones reached or, if missed, an explanation provided;

(b) Any problems or delays encountered or anticipated and recommendations for resolution. If the recommended resolution involves a contract modification, e.g., change in work requirements, level of effort (cost) or schedule delay, the contractor shall submit a separate letter to the contracting officer identifying the required change and estimated cost impact.

(c) A summary of progress to date; and

(d) Plans for the next reporting period.

A.23 2052.211-72 FINANCIAL STATUS REPORT (OCT 1999)

The contractor shall provide a monthly Financial Status Report (FSR) to the project officer and the contracting officer. The FSR shall include the acquisition of, or changes in the status of, contractor-held property acquired with government funds valued at the time of purchase at \$50,000 or more. Whenever these types of property changes occur, the contractor shall send a copy of the report to the Chief, Property and Acquisition Oversight Branch, Office of Administration. The report is due within 15 calendar days after the end of the report period and must identify the title of the project, the contract number, the appropriate financial tracking code (e.g., Job Code Number or JCN) specified by the NRC Project Officer, project manager and/or principal investigator, the contract period of performance, and the period covered by the report. Each report must include the following for each discrete task:

(a) Total estimated contract amount.

(b) Total funds obligated to date.

(c) Total costs incurred this reporting period.

(d) Total costs incurred to date.

(e) Detail of all direct and indirect costs incurred during the reporting period for the entire contract or each task, if it is a task ordering contract.

(f) Balance of obligations remaining.

(g) Balance of funds required to complete contract/task order.

(h) Contractor Spending Plan (CSP) status: A revised CSP is required with the Financial Status Report whenever the contractor or the contracting officer has reason to believe that the total cost for performance of this contract will be either greater or substantially less than what had been previously estimated.

(1) Projected percentage of completion cumulative through the report period for the project/task order as reflected in the current CSP.

(2) Indicate significant changes in the original CSP projection in either dollars or percentage of completion. Identify the change, the reasons for the change, whether there is any projected overrun, and when additional funds would be required. If there have been no changes to the original NRC-approved CSP projections, a written statement to that effect is sufficient in lieu of submitting a detailed response to item "h".

(i) Property status:

(1) List property acquired for the project during the month with an acquisition cost between \$500 and \$49,999. Give the item number for the specific piece of equipment.

(2) Provide a separate list of property acquired for the project during the month with an acquisition cost of \$50,000 or more. Provide the following information for each item of property: item description or nomenclature, manufacturer, model number, serial number, acquisition cost, and receipt date. If no property was acquired during the month, include a statement to that effect. The same information must be provided for any component or peripheral equipment which is part of a "system or system unit."

(3) For multi-year projects, in the September monthly financial status report provide a cumulative listing of property with an acquisition cost of \$50,000 or more showing the information specified in paragraph (i)(2) of this clause.

(4) In the final financial status report provide a closeout property report containing the same elements as described above for the monthly financial status reports, for all property purchased with NRC funds regardless of value unless title has been vested in the contractor. If no property was acquired under the contract, provide a statement to that effect. The report should note any property requiring special handling for security, health, safety, or other reasons as part of the report.

(j) Travel status: List the starting and ending dates for each trip, the starting point and destination, and the traveler(s) for each trip.

(k) If the data in this report indicates a need for additional funding beyond that already obligated, this information may only be used as support to the official request for funding required in accordance with the Limitation of Cost (LOC) Clause (FAR 52.232-20) or the Limitation of Funds (LOF) Clause FAR 52.232-22.

A.24 2052.215-70 KEY PERSONNEL (JAN 1993)

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



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

(b) If one or more of the key personnel, for whatever reason, becomes, or is expected to become, unavailable for work under this contract for a continuous period exceeding 30 work days, or is expected to devote substantially less effort to the work than indicated in the proposal or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the 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.25 PROJECT OFFICER AUTHORITY ALTERNATE 2 (FEBRUARY 2004)

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

Name: Andrew Welkie
Address: US NRC
Mail Stop: T3-F23
Washington DC 20555
Telephone Number: 301-415-6541
Email: Andrew.welkie@nrc.gov

(b) The project officer shall:

(1) Place delivery orders for items required under this contract up to the amount obligated on the contract award document.

NRC-DR-21-10-496

(2) Monitor contractor performance and recommend changes in requirements to the contracting officer.

(3) Inspect and accept products/services provided under the contract.

(4) Review all contractor invoices/vouchers requesting payment for products/services provided under the contract and make recommendations for approval, disapproval, or suspension.

(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.

(c) The project officer may not make changes to the express terms and conditions of this contract.

A.26 2052.215-78 TRAVEL APPROVALS AND REIMBURSEMENT -ALTERNATE 1 (OCT 1999)

(a) Total expenditure for travel may not exceed \$101,212 without the prior approval of the contracting officer. This amount include domestic and local travel and the applicable general and administrative charges related to this travel.

(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.

A.27 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

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

A.28 PROJECT SUPPORT CONTRACTORS

The Government may either award or have awarded management, engineering, technical, and other professional

support service contracts (hereafter referred to as Project Support Contractors). Project Support Contractors may require access to proprietary and other data relating to technical matters (including cost and schedule) concerning this contract to the same degree such access is accorded Government personnel.

The Contractor shall cooperate with Project Support Contractors by engaging in technical discussions with Project Support Contractors' personnel, and permitting such personnel access to information and data relating to technical matters (including cost and schedule) concerning this contract to the same degree such access is accorded Government personnel.

Project Support Contractors shall agree to protect proprietary information of the Contractor in accordance with Federal Acquisition Regulation (FAR) 9.505-4, to not engage in the production of products (including software), and to otherwise abide by FAR Subpart 9.5, entitled "Organizational Conflicts of Interest." Project Support Contractors shall be required to directly execute nondisclosure, non-use agreements with the Contractor and subcontractors if so requested by the Contractor.

A.29 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

(a) The following representation is required by the NRC Acquisition Regulation 2009.105-70(b). It is not NRC policy to encourage offerors and contractors to propose current/former agency employees to perform work under NRC contracts and as set forth in the above cited provision, the use of such employees may, under certain conditions, adversely affect NRC's consideration of non-competitive proposals and task orders.

(b) There () are () are no current/former NRC employees (including special Government employees performing services as experts, advisors, consultants, or members of advisory committees) who have been or will be involved, directly or indirectly, in developing the offer, or in negotiating on behalf of the offeror, or in managing, administering, or performing any contract, consultant agreement, or subcontract resulting from this offer. For each individual so identified, the Technical and Management proposal must contain, as a separate attachment, the name of the individual, the individual's title while employed by the NRC, the date individual left NRC, and a brief description of the individual's role under this proposal.

A.30 LIST OF ATTACHMENTS

1. Price schedule
2. Statement of work
3. NRC-35
4. Billing instructions
5. NRC-187

Summary of all tasks and years

Task Number	Task Title	Contract Type	Base Year	OP 1	OP2	OP3	OP4	Total all years
Task 1	Operations and Maintenance (General, daily and weekly tasks):	FFP	\$ 177,449.74	\$ 185,180.24	\$ 192,255.99	\$ 199,293.14	\$ 206,598.16	\$ 960,777.25
Task 1a	Operations and Maintenance "As needed tasks"	T&M	\$ 241,784.81	\$ 256,900.09	\$ 272,505.81	\$ 288,949.64	\$ 306,663.28	\$ 1,366,803.63
Task 2	IT Security Related Activities	T&M	\$ 168,922.19	\$ 176,209.29	\$ 156,196.20	\$ 148,096.30	\$ 153,455.72	\$ 802,879.70
Task 3	Hearing / Meeting Support	T&M	\$ 522,289.84	\$ 788,949.98	\$ 807,414.43	\$ 835,054.22	\$ 447,091.19	\$ 3,400,799.65
Task 4	Application Enhancements, Development and Test Environment	T&M	\$ 258,497.14	\$ 269,463.38	\$ 279,619.29	\$ 289,736.17	\$ 333,832.15	\$ 1,431,148.13
Task 5 - see note	Training	FFP per training Session	\$ 87,592.26	\$ 90,629.51	\$ 93,396.26	\$ 96,160.26	\$ 99,029.76	\$ 466,808.06
Optional Task 6a	Technology Refresh of Rockville Data Processing sub-system	T&M	\$ -	\$ -	\$ -	\$ 160,803.32	\$ -	\$ 160,803.32
Optional Task 6b	Technology Refresh of Las Vegas Data Processing sub-system	T&M	\$ -	\$ -	\$ -	\$ -	\$ 57,189.61	\$ 57,189.61
Optional Task 6c	Technology Refresh of Rockville Audio Visual Sub-System	T&M	\$ -	\$ -	\$ -	\$ 177,852.68	\$ -	\$ 177,852.68
Optional Task 6d	Technology Refresh of Las Vegas Audio Visual Sub-System	T&M	\$ -	\$ -	\$ -	\$ -	\$ 193,829.67	\$ 193,829.67
Optional task 7	Transition Task	FFP	\$ -	\$ -	\$ -	\$ -	\$ 145,165.44	\$ 145,165.44
Total			\$ 1,456,535.98	\$ 1,767,332.48	\$ 1,801,387.97	\$ 2,195,945.72	\$ 1,942,854.98	\$ 9,164,057.14



Digital Data Management System

Statement of Work

Digital Data Management System
Operations and Maintenance Statement of Work

Table of Contents

1 Background	1
1.1 Available Documentation	3
1.2 Acronyms	6
2 Objective	7
3 Scope	7
4 Definitions	9
5 Tasks	10
5.1 Task One – Operations and Maintenance.....	10
5.1.1 Scope of Maintenance Activity	10
5.1.2 Objectives.....	13
5.1.3 Initiation of Work	13
5.1.4 Work Actions Requiring Pre-Approval	14
5.1.5 Standard Work Approach.....	14
5.1.6 Specialized Maintenance Support.....	15
5.1.7 Scheduled Deliverables	15
5.2 Task Two – IT Related Security Activities	16
5.2.1 Objectives.....	16
5.2.2 Scope of Security Activity.....	16
5.2.3 Initiation of Work	19
5.2.4 Scheduled Deliverables	19
5.3 Task Three – Hearing/Meeting Support	20
5.3.1 Objectives.....	20
5.3.2 Scope of Hearing/Meeting Support	20
5.3.3 Initiation of Work	21
5.3.4 Scheduled Deliverables	22
5.4 Task Four – Application Enhancements, Development and Test Environment	22
5.4.1 Objectives.....	22
5.4.2 Scope of Application Enhancements Activity.....	22
5.4.3 Scope of Test Environment Activity.....	23
5.4.4 Initiation of Work	24
5.4.5 Scheduled Deliverables	24
5.5 Task Five – Training	24
5.5.1 Objectives.....	24
5.5.2 Scope of Training Activity.....	24
5.5.3 Initiation of Work	25
5.5.4 Scheduled Deliverables	25
5.6 Optional Tasks.....	25
5.6.1 Optional Task 6A - Technology Refresh of Rockville Data Processing Sub-System.....	25
5.6.2 Optional Task 6B - Technology Refresh of Las Vegas Data Processing Sub-System.....	27

Digital Data Management System
Operations and Maintenance Statement of Work

5.6.3 Optional Task 6C - Technology Refresh of Rockville Audio/Visual Sub-System.....	28
5.6.4 Optional Task 6D - Technology Refresh of Las Vegas Audio Visual Sub-System.....	30
5.7 Optional Tasks - Estimated Period of Performance and Delivery Schedule	31
6 Optional Task Seven - Transition Task	33
6.1 Objective	33
6.2 Scope of Transition Task	33
6.3 Initiation of Work.....	33
7 NRC Computer Security Requirements.....	33
8 Meetings and travel	36
9 Period of Performance	36
10 Place of Performance.....	36
11 Contractor Performance Requirements.....	36
11.1 Documentation Deliverables	36
11.2 Quality Assurance Surveillance Plan	37
11.2.1	Purpose of the QASP 37
11.2.2	Types of Work Performed 37
11.2.3	Methods of Surveillance 38
11.2.4	Quality Assurance Forms and Report 38
11.2.5	Analysis of Surveillance Results 39

Digital Data Management System Operations and Maintenance Statement of Work

1 Background

The Atomic Safety and Licensing Board Panel (ASLBP) conducts all licensing and other hearings as directed by the Commission, primarily through individual three-judge Atomic Safety and Licensing Boards appointed by either the Commission or the Chief Administrative Judge. In addition to adjudicating licensing and enforcement cases regarding nuclear power reactors and nuclear materials, ASLBP is responsible for conducting the adjudicatory proceeding regarding the Department of Energy's (DOE) application for construction authorization for a high-level waste (HLW) repository at Yucca Mountain, NV. The scope and nature of that proceeding, as well as the agency's other reactor and materials licensing adjudications, dictate the essential need for efficient capture and management of the enormous volume of multimedia data that must be processed and displayed in a very short time frame.

The U.S. Nuclear Regulatory Commission (NRC) established digital information retrieval, utilization, and display capabilities in conjunction with the potential licensing proceeding for a HLW repository with the Digital Data Management System (DDMS), which has been successfully developed and deployed in the NRC Two White Flint North (TWFN) complex in Rockville, MD and in a GSA-leased building in Las Vegas.

Because judges and judicial law clerks, lawyers and other party representatives, and technical support staff will use the DDMS interchangeably in both Rockville and Las Vegas in support of the Yucca Mountain proceeding, as well as other proceedings, the components installed in the Las Vegas facility are basically identical to those installed in Rockville. Additionally, data and document files stored in the Rockville system must be made available to support hearings held in Las Vegas, and vice versa, driving a requirement that the databases and data files under this effort be a virtual mirror image in both locations.

The DDMS combines web-based document management with digital evidence presentation/recording to provide users with access to searchable evidentiary material, including video transcripts and a means to present most evidentiary material electronically. Although primarily a system for litigants, the DDMS also provide the public with greater public access to ASLBP hearings by providing large-screen monitors display of evidentiary materials and internet-available web broadcasts of hearing sessions. DDMS also permits greater access for disabled persons by providing closed-captioning, assisted listening, and compatibility with computer screen-reading technology. Because the system was developed using a standard web interface, users can access DDMS from the ASLBP Rockville, Maryland hearing room, the ASLBP Las Vegas, Nevada hearing facility, a "remote" hearing site, or wherever they are able to establish an Internet connection.

Specifically, DDMS:

- A. Provides information technology (IT) and audio/visual (A/V) capabilities in the ASLBP's Rockville and Las Vegas hearing rooms and, potentially, other "remote" locations where hearings are conducted;
- B. Enables the creation and use of an integrated, comprehensive digital record for agency licensing and enforcement cases;
- C. Records, stores, and displays the text and image of documents presented in a hearing using pre-filed electronic documents from the agency's Electronic Hearing Docket (EHD);

Digital Data Management System Operations and Maintenance Statement of Work

- D. Permits access and retrieval of the entire record of a case, including (1) already docketed documentary material, transcripts, and exhibits; (2) previously recorded A/V presentations or computer simulations; and (4) hearing session testimony;
- E. Allows counsel for the parties to bring electronically prepared evidentiary material to the hearing and have it integrated into the record and accessible in the hearing room;
- F. Provides almost continual, virtually real-time access to the hearing record by the presiding officer and parties to the litigation;
- G. Supports prehearing, hearing, and post-hearing information management (IM) for the trial-level Licensing Board proceeding and any subsequent agency and judicial appellate processes;
- H. Is consistent with the Commission's procedural rules and policies;
- I. Enhances the ability of the Licensing Board and the litigants to conduct efficient and effective hearings;
- J. Provides enhanced public access to information used during the hearing; and
- K. Improves litigant and public perceptions of the NRC adjudicatory process.

DDMS improves the ability of the NRC to conduct business electronically with external entities and employs techniques to process and make available electronically the entire record of an adjudicatory proceeding, thereby reducing paper and manual processes. The system also employs teleconference and videoconference technologies to make Board member, NRC staff, witness, and party participation more flexible. Additionally, it provides external stakeholders with the ability to access the agency's publicly available information more easily and effectively.

The DDMS is comprised of three main subsystems.

Hearing Management

The DDMS Hearing Management subsystem administers, at a high level, the information associated with the hearing itself. This includes calendaring, scheduling, report generators, and other functions related to hearing management. Other functions include capturing dispositional information, along with managing and linking lists and other information about witnesses, depositions, exhibits, and issues. Finally, the hearing management software securely manages documents covered under a protective order in such a way as to prevent tampering and unauthorized disclosure.

Document/Object Management

The DDMS Document/Object Management subsystem is implemented using web-based portal technology. Additionally, Microsoft SQL Server is used to manage the documents and objects within the DDMS. Through the DDMS portal - which provides the primary user interface - users can locate any document within the DDMS according to their access permission. The Document/Object Management subsystem also maintains a listing of each day's proceeding activity. This includes object (exhibit) references, the official transcript, scheduled and actual witness appearances, the video file, and other documents pertaining to the hearing.

The Web/Portal Server (supporting the Document/Object Management subsystem) hosts the interfaces between the DDMS and the rest of the NRC. These include interfaces with the agency's ADAMS document management system, thereby allowing the DDMS to receive pre-filed materials submitted to the NRC via the agency's Electronic Information Exchange (EIE)/E-Filing server. The DDMS Web/Portal Server also provides users an interface to limited external internet sites such as Lexis/Nexis, Westlaw, the Licensing Support Network, and the NRC's official web site. Through this interface point, internal DDMS users are allowed access to these

Digital Data Management System Operations and Maintenance Statement of Work

pre-defined services in a secure environment in which the specific sites that users can utilize are constrained through the use of IP filtering on the DDMS boarder routers. These latter functions, while characterized as Document/Object Management, also support the Hearing Management environment.

Multimedia Management

A hearing's live video feed is routed into a video switcher. The switcher is sound activated to provide automatic camera switching to capture the current speaker. In the event that a clerk needs to manually switch camera views, an override capability is provided to allow for manual camera switching. The system is also configured such that the audio can be either automatically or manually switched with a manual override/muting capability.

The composite output of the switched video feed is routed to the indexing and encoding subsystem where it is synchronized with the real-time text transcript feed from the court reporter. Following indexing, the DDMS encoding feature converts the composite video feeds to digital video for storage in the video server and storage subsystems.

The digital video is stored in the video server and storage subsystem in Windows Media Video format. The video server and storage subsystem also contains a transcoding system and streaming media server(s) to allow for low-resolution viewing of video to authorized DDMS users accessing the system from the hearing room or over the internet.

a. Available Documentation

The following documents¹ describe the operational state of DDMS:

Table 1-1 - DDMS Documentation

Document Title	Document Description
DDMS Backup and Recovery Plan	This document provides a comprehensive description of the backup and recovery plan and procedures for DDMS.
DDMS Change Control Board Charter	The DDMS Change Control Board charter describes the board's objectives, scope, membership, roles and responsibilities of members, reporting and approval process (including standard and emergency changes), meeting frequency, and relationship to other boards.
DDMS Configuration Management Plan	The Configuration Management Plan (CMP) describes the approach and processes for managing and versioning configuration items created for DDMS. The CMP is part of an overall quality control program that promotes quality development and deployment of the application and underlying infrastructure. The intended audiences for this document are ASLBP Management, DDMS Project Team, DDMS Change Control Board Members, and the DDMS Operations and Maintenance contractor.
DDMS Contingency Plan	The purpose of the DDMS Contingency Plan is to define the process and procedures to be followed to recover and restore the operation of the DDMS in the most effective and efficient manner should severe failures occur within the DDMS itself or within the overall infrastructure required to support DDMS operations.
DDMS Failover Procedures	Documented procedures used to recover from failures that cause the execution of the Contingency Plan
DDMS Incident Response Plan	The Purpose of the Digital Data Management System Incident Response Plan is to define the process and procedures for preparing, detecting, containing, eradicating, recovering from computer security incidents as well as reporting incidents properly.

¹ DDMS documentation is updated on a regular basis. DDMS maintains an authoritative source of documentation in its DDMS Table of Documents document

**Digital Data Management System
Operations and Maintenance Statement of Work**

Document Title	Document Description
DDMS Interface Control Document	The purpose of the Interface Control Document (ICD) is to provide a reference for the mechanism of data flow through the system and a detailed identification of the security controls applied. The ICD includes details related to user-to-system (User Interfaces) and system-to-system (System Interfaces) based interfacing. Information such as triggering mechanisms, network paths, network interconnectivity, network addressing, and TCP/UDP ports are contained within this document.
DDMS IT Security Procedures	This document is intended to provide information, documentation and references regarding all facets of the security program for the DDMS. This includes the information technology policies and procedures that ensure compliance with the National Institute of Standards and Technology guidelines applicable to security and safe operation of Federal Government computer systems. This also addresses issues of personnel security and information management as outlined by the NRC Management Directives (MD) 12.1 and 12.3. In addition this document describes the procedures in place to address physical security issues as outlined in the NRC MD 12.1 and the "Las Vegas Hearing Facility Security Plan". Finally, site specific issues regarding emergency procedures, in conjunction with the Occupant Emergency Plans (OEP) for both Rockville and Las Vegas as it pertains to the DDMS installations is covered.
DDMS Operations Guide	<p>The Operations Guide (9 Chapters) provide instructions for Clerks and Administrators, and acts a roadmap for the operational aspects and the configuration of DDMS, its components and processes. This guide provides the guidance and procedures necessary for experienced staff to effectively assist DDMS personnel in managing DDMS processes and assisting ASLBP business processes. With this guide, DDMS personnel will be able to run and manage routine Portal jobs, perform event-driven DDMS procedures, conduct routine administration of the servers and software, perform timely backups, retrieve and restore data from backup media, and recover the system from failures and errors.</p> <p>The Operations Guide is intended to provide detailed documentation to DDMS personnel, providing guidance and procedures to effectively operate the system or configure components, should the need arise. This guide is the reference handbook for DDMS personnel.</p>
DDMS Participant User Guide	<p>The objective of this Participant Users Guide is to provide DDMS users with enough instruction to be able to efficiently use the system. DDMS will be utilized by a wide variety of users. It is important that this User Guide be available to all users concurrent with the training and/or use of DDMS. This User Guide encompasses all DDMS user groups and all organizations responsible for maintaining and administering the system. This includes: ASLBP staff with primary system sponsorship responsibilities; internal NRC users such as the Office of General Counsel; all other parties to the HLW licensing hearings; and the system and database Administrators.</p> <p>While the training materials are designed to focus on specific user groups, this manual is intended to be used by all users, regardless of role. In addition, many of the Clerk-specific and Administrator-specific tasks are shown in more detail in the Operations Guide.</p>
DDMS Production Design Document	This document describes the original design for the DDMS to be used in conducting the HLW licensing proceeding in the Las Vegas, Nevada and Rockville, Maryland hearing facilities.

Digital Data Management System
Operations and Maintenance Statement of Work

Document Title	Document Description
DDMS Risk Assessment Detail and narrative	This security risk assessment follows the guidance from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, <i>Risk Management Guide for Information Technology Systems</i> and U.S. Nuclear Regulatory Commission (NRC) Management Directive 12.5, <i>NRC Automated Information Systems Security Program</i> . Its purpose is to evaluate and document the extent to which safeguards or countermeasures, as prescribed within the NIST SP 800-53 and hereafter referred to as security controls, are in place and operating as intended, such that the information stored, processed, and transmitted by the DDMS is adequately secured and protected. The risk assessment characterizes system threats and vulnerabilities, including the likelihood of each threat-source exploiting the associated vulnerability, and then determines the potential harm or impact each threat/vulnerability pair and associated threat action could impose upon the confidentiality, integrity, and availability of system information in the event a security control is not properly implemented. The resulting product of the likelihood and the impact associated with a given threat/vulnerability pair is the risk for that particular pair.
DDMS Roles and Responsibilities	The purpose of the DDMS Roles and Responsibilities document is to provide an overview of the DDMS personnel roles, sensitivity criteria, corresponding access authorizations, and training requirements. It describes what actions each role can perform at an application and/or system level. Additionally it provided contact information for all personnel holding a DDMS role.
DDMS Rules of Behavior	The purpose of this document is to explain to all authorized DDMS users the Rules of Behavior and requirements as specified by OMB Circular A-130, NRC Information Security Guidance, and other related policies. As the property of the Federal Government, the DDMS, including its software, hardware, and the information it contains, must be protected from damage resulting from misuse by authorized and unauthorized users. Users' access to the DDMS reflects a high level of trust accorded to the participants in an Atomic Safety and Licensing Board Panel (ASLBP or the Panel) proceeding by the Panel. Specifically, by granting access to the system, the Panel is placing trust in authorized users that they will not misuse the system or allow it to be misused by others. These Rules of Behavior are intended to ensure that authorized users are aware of their responsibilities when using DDMS.
DDMS Security Categorization	The purpose of the DDMS Security Categorization is to define and document the security category for the system. This security categorization establishes the foundation of the certification and accreditation of the DDMS information system by determining the levels of rigor required for certification and overall assurance testing of security controls, as well as additional activities that may be needed. Thus, it assists in determining the level of effort required for certification and accreditation and the associated activity duration. Security categorization is a prerequisite activity for the certification and accreditation process. This categorization should be revisited at least every three years or when a significant change occurs to the system or supporting business lines. Situational changes outside the system or agency may require a reevaluation of the categorization (e.g., directed mission changes, changes in governance, elevated or targeted threat activities).
DDMS Security Test & Evaluation Plan	The purpose of the DDMS Security Test & Evaluation (ST&E) is to determine compliance with the security requirements documented in the DDMS System Security Plan (SSP) and to verify that the security controls identified in the SSP are correctly implemented and effective. The purpose of the ST&E plan is to provide a plan for an effective and adequate ST&E. It provides a high-level overview of the system operating environment, the approach and schedule for testing, the nature and extent of the testing, and the ST&E team composition, and provides the methodology assessing the security controls for the system.

Digital Data Management System Operations and Maintenance Statement of Work

Document Title	Document Description
DDMS Software Engineering Notebook	The Software Engineering Notebook compiles and centralizes developer information relating to the DDMS application and complies with the NRC System Development and Life Cycle Management (SDLCM) requirements for the Software Engineering Notebook.
DDMS System Security Plan	In accordance with the provisions of FISMA, information security programs are required to have plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate. The preparation of a security plan for an information system ensures that agreed upon security controls planned or in place are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones).
DDMS Training Plan	The objectives of this Training Plan are multi-faceted. Because DDMS will be utilized by a wide variety of users, it is imperative that a strong training program accompanies the implementation of the system. This Plan documents the methods and procedures needed to ensure that DDMS users are capable of fully utilizing the functionality of the system and employing its capabilities to add efficiencies to the ASLBP proceedings.
Las Vegas Audio Visual Operations Guide	The purpose of the manual is to provide the reader with a comprehensive description of the electronic audio, video, and control systems integrated into the Las Vegas hearing room. The manual details the essential operating and maintenance information required by court personnel to manage the integrated system.
Rockville Audio Visual Operations Guide	The purpose of the manual is to provide the reader with a comprehensive description of the electronic audio, video, and control systems integrated into the Rockville hearing room. The manual details the essential operating and maintenance information required by court personnel to manage the integrated system.

Note: All documents listed in the above table will be provided on compact disk, or other appropriate medium, in Portable Document Format (PDF) to interested Offerors. PDF security settings will be enabled and Adobe Reader 9.0 will be required to view these documents that, as is the case with many DDMS documents, are considered sensitive security information and are thus categorized as sensitive unclassified non-safeguards information (SUNSI).

b. Acronyms

AV	Audio/Visual
ADAMS	Agencywide Documents Access and Management System
ASCII	American Standard Code for Information Interchange
ASLBP	Atomic Safety and Licensing Board Panel
CCB	Configuration Control Board
CNSS	Committee on National Security Systems
COTS	Commercial Off the Shelf
CSO	Computer Security Office
CTF	Consolidated Test Facility
DFS	Division of Facility Security
DOE	Department of Energy

Digital Data Management System Operations and Maintenance Statement of Work

EHD	Electronic Hearing Docket
EIE	Electronic Information Exchange
ET	Eastern Time
EV	Earned Value
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HLW	High Level Waste
IT	Information Technology
DDMS	Digital Data Management System
LAN	Local Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
O&M	Operations and Maintenance
OIS	Office of Information Services
OS	Operating System
PDF	Portable Document Format
PMM	Project Management Methodology
POE	Production Operating Environment
QA	Quality Assurance
RUP	Rational Unified Process
SB	Security Branch
SQL	Structured Query Language
SUNSI	Sensitive Unclassified Non-Safeguards Information
TAE	Test and Acceptance Environment
TWFN	Two White Flint North
UML	Unified Modeling Language
WAN	Wide Area Network

2 Objective

The objective of this contract is to provide the NRC and, more specifically, the Atomic Safety and Licensing Board, with both specialized operations and maintenance (O&M) support for the DDMS and day-to-day hearing support. DDMS must remain operational to support the highly visible and contentious HLW proceeding as well as other ASLBP hearings or meetings held at the Rockville hearing room, the Las Vegas hearing facility, or other hearing sites throughout the United States and its territories.

3 Scope

The Contractor shall provide all necessary personnel and materials required in support of the tasks outlined in this statement of work. Specifically, the Contractor shall provide:

- Operations and maintenance support for the DDMS installations at
 - the Rockville hearing room,
 - the Las Vegas hearing facility
- Application installations in
 - the Consolidated Test Facility (CTF),
 - Test and Acceptance Environment (TAE), and/or
 - Contractor development lab.
- Day-to-day hearing support for hearings held at

Digital Data Management System Operations and Maintenance Statement of Work

- the Rockville Hearing room
- the Las Vegas Hearing Facility, and
- Remote locations or other hearing sites throughout the United States and its territories.

The Contractor shall be responsible for the maintenance of all visual and data processing components installed at the NRC HQ hearing room and the Las Vegas hearing facility.

The Contractor shall be responsible for notifying the NRC DDMS Project Officer of the expiration of any software or hardware maintenance agreements that are tracked in the DDMS inventory database².

The Contractor shall comply with the latest version of all applicable Federal and Agency IT Security policy, guidance and standards. These policy, guidance and standards include, but are not limited to:

- DDMS IT Security Documentation (see Table 1-1);
- NRC Policies, Procedures, and Standards³ such as:
 - NRC Agency-wide Rules of Behavior for Authorized Computer Use
 - NRC Data at Rest Encryption Policy;
 - NRC Sensitive Unclassified Non-Safeguards Information (SUNSI);
 - Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities;
 - Computer Security Information Protection Policy;
 - Remote Access Policy
 - Use of Commercial Wireless Devices, Services and Technologies
 - Laptop Security Policy
 - Computer Security Incident Response Policy
 - NRC Continuous Monitoring Program
 - NRC Plan of Action & Milestones Process
- All applicable NRC Management Directives⁴ (MD) such as
 - MD 12.5 Automated Information Security Program;
 - MD 12.6 NRC Sensitive Unclassified Information Security Program;
- National Institute of Standards and Technology (NIST) Special Publications (SP)⁵;
- NIST Federal Information Processing Standards (FIPS)⁶; and
- The Committee on National Security Systems (CNSS⁷) policy, directives, instructions, and guidance.

² The DDMS inventory database is a Microsoft Access database that contains detailed information regarding the DDMS hardware and software components.

³ Any applicable NRC policies, procedures, or standards will be provided on compact disk, or other appropriate medium, in PDF to interested Offerors. PDF security settings will be enabled and Adobe Reader 9.0 will be required to view these documents

⁴ NRC Management Directives can be found on the NRC's website (<http://www.nrc.gov/reading-rm/doc-collections/management-directives/>). MD 12.5 is only available in redacted form and its full version will be provided on compact disk, or other appropriate medium, in PDF to interested Offerors. PDF security settings will be enabled and Adobe Reader 9.0 will be required to view these documents.

⁵ NIST SP can be found at the following web site: <http://csrc.nist.gov/publications/PubsSPs.html>

⁶ NIST FIPS can be found at the following web site: <http://csrc.nist.gov/publications/PubsFIPS.html>

⁷ The website for The Committee on National Security Systems is <http://www.cnss.gov/>

Digital Data Management System Operations and Maintenance Statement of Work

4 Definitions

Application maintenance is defined as the modification, correction or installation of updates to NRC owned code and/or NRC owned data following appropriate DDMS configuration management procedures, which are part of the DDMS application system intended to support ASLBP business processes. These modifications/corrections include, but are not limited to, modification of programs, portlets, table structures, data, and documentation.

Maintenance also includes, but is not limited to, the analysis of conditions and outputs to identify root causes of problems and define methods for correcting, troubleshooting, establishing, and executing project-level configuration management; backups; restores; archives; housekeeping (i.e., keeping a control room neat and organized, labeling equipment and/or cabling); the installation of vendor-supplied software patches and maintenance releases in conformance with the appropriate software licenses; and coordination with software and hardware vendors to identify and track open "tickets" for resolving and closing software technical issues.

Operating environment maintenance is defined as servers, their operating systems and associated software, and all software components not embedded in the application software defined in the DDMS Operations Support Guide.

Operational support is defined as data support, report generation, and application support.

Data support shall include, but is not be limited to, data interpretation, discrepancy resolution, and verification.

Report generation shall include producing from DDMS in various output formats, including hard copy and electronic (Microsoft Word, ASCII, Microsoft Excel, PDF, etc.), either on a scheduled or ad-hoc basis: (a) standard reports, (b) quick queries, or (c) new reports using newly defined criteria. This includes the development of additional "canned" queries and reports as identified by the NRC DDMS Project Officer.

Production support shall include, but is not be limited to, initiating program sequences on a prescribed schedule; Quality Assurance (QA) reviews and data transfers between systems through either kick-off of electronic processes (programs) or inputs of tapes or other physical media; and system monitoring, troubleshooting, and immediate corrective measure implementation for agency production application systems.

Hearing support shall include, but is not be limited to, the operation and maintenance of evidence presentation systems, electronic stamping of exhibits, presentation of electronic evidence, and processing of electronic ad hoc documents.

Digital Data Management System Operations and Maintenance Statement of Work

5 Tasks

5.1 Task One – Operations and Maintenance

1.1.1 Scope of Maintenance Activity

1. General Tasks

The Contractor shall adhere to the NRC's PMM⁸ approach for all activities performed under this contract.

The Contractor, following configuration management procedures defined in the DDMS Configuration Management Plan, shall be responsible for making necessary changes to ensure that corrective, adaptive and perfective requirements are implemented accurately and are fully documented.

The Contractor shall ensure that all software usage meets Federal copyright laws and that the appropriate number of licenses is maintained and tracked for the software utilized in the operation of the DDMS as detailed in the DDMS Inventory database to include, but not be limited to: Operating System (OS) software, Commercial off the Shelf (COTS) software packages, including application software, database software, and security/virus detection software including digital signatures software. The Contractor shall provide a report on the first day of each quarter that details any software or hardware license or maintenance agreements that will expire during the following quarter.

The Contractor shall maintain all DDMS application database tables, including SQL Server and Plumtree tables, following procedures documented in the DDMS Operational Support Guide Manual. This may include posting changes that result from minor data normalization and cleanup activities as the size of the DDMS databases increase.

All Contractors holding a DDMS role, as defined in the DDMS Roles and Responsibilities document, shall meet the required competencies and requisite training detailed in that document. Should the required capabilities or training change for a particular role, the NRC DDMS Project Officer will notify the Contractor of the change and the Contractor shall have nine (9) months from the time of notification to ensure that all Contractors holding a DDMS role meet the required competencies and requisite training. All Contractor staff training, unless specific to NRC operations, offered by the NRC and is required for all NRC employees and NRC Contractors, shall be at the Contractor's expense.

On the first business day of each calendar year quarter, the Contractor shall provide the DDMS Project Team with a list of training completed by Contractor staff during that quarter that will include the staff member's name, the course title, and the course completion date. At the same time, the Contractor shall also provide a list of scheduled staff member training for the upcoming quarter, to include the staff member's name, the course title, and the scheduled date.

⁸ The NRC's PMM approach is described in Management Directive 2.8 and is available at the following website: <http://www.nrc.gov/reading-rm/doc-collections/management-directives/volumes/vol-2.html>.

Digital Data Management System Operations and Maintenance Statement of Work

2. Daily Tasks

The Contractor shall ensure that, on a daily basis by no later than 8:30 a.m. Eastern Time (ET) (unless directed otherwise by the NRC DDMS Project Officer and excluding weekends and Federal holidays), any documents published from ADAMS to DDMS have been indexed into DDMS and that all newly-indexed metadata is correct in accordance with the procedures documented in the DDMS Operations Support Guide. Should there be an indexing problem, the Contractor shall take corrective action following the procedures documented in the DDMS Operations Support Guide and will notify the DDMS Project Management Team immediately. Should the corrective actions taken not resolve the indexing problem, the Contractor shall not take no further action until directed by the NRC DDMS Project Officer.

The Contractor shall ensure that, on a daily basis by no later than 8:30 a.m. ET (unless directed otherwise by the NRC DDMS Project Officer and excluding weekends and Federal holidays), in accordance with the procedures documented in the DDMS Operations Support Guide, any documents entered into DDMS as ad hoc documents (i.e., those which have not been prefiled via EIE/E-Filing) have been transferred and are available in ADAMS⁹. Should there be a problem, the Contractor shall notify the DDMS Project Management Team and database administrators for other impacted systems immediately and remain available for further action as required.

The Contractor shall, on a daily basis by no later than 8:30 a.m. ET (unless directed otherwise by the NRC DDMS Project Officer and excluding weekends and Federal holidays), record, in a government-furnished Microsoft Access database available on the NRC LAN, the environmental status, to include temperature and humidity readings, of the Rockville A/V room, Las Vegas A/V room, and Las Vegas IT Room using a government furnished environmental monitoring device as defined in the DDMS IT Security Procedures Document.

The Contractor shall confirm that, on a daily basis by no later than 8:30 a.m. ET (unless directed otherwise by the NRC DDMS Project Officer and excluding weekends and Federal holidays), the previous night's data backup was successful and relay any negative results to DDMS Project Management Team together with a plan for resolution following procedures documented in the DDMS Backup and Recovery Plan.

The Contractor shall ensure that connectivity is maintained between the DDMS installation in the Rockville hearing room and the Las Vegas facility, as well as connectivity to the Internet and to other NRC systems.

The Contractor shall (1) ensure that SQL Server Database replication is functioning, file system replication is functioning, and scheduled application processes have initiated and completed successfully; and (2) troubleshoot NRC Local Area Network (LAN) and Wide Area Network (WAN) connectivity problems working in conjunction with OIS as directed by the NRC DDMS Project Officer.

⁹ The process for documents being transferred to DDMS from ADAMS or from DDMS to ADAMS is available in the DDMS Interface Control Document.

Digital Data Management System Operations and Maintenance Statement of Work

3. Weekly Tasks

The Contractor shall perform server operating system and application software diagnostics as detailed in the DDMS Operations Support Guide at least once every week. The Contractor shall deliver a report detailing the results of the weekly diagnostic tests to the DDMS Project Management Team via the DDMSwebmaster@nrc.gov e-mail account using the internal NRC e-mail system.

4. As Needed Tasks

The Contractor shall provide support to ASLBP staff, on an as-needed basis, in connection with the process for covert paper copy exhibits to electronic documents utilizing government furnished equipment.

The Contractor shall be responsible for ensuring that all servers, workstations, routers, firewalls, and their operating systems are patched to the current recommended versions. The Contractor shall provide all testing, including regression testing, that may be required per the configuration control procedures outlined in the NRC's PMM procedures, the DDMS Configuration Control Board (CCB) procedures, and the DDMS Configuration Management Plan, by following the procedures documented in the DDMS Operational Support Guide and the DDMS Security Guidelines document. All patch installations shall be pre-coordinated with the NRC DDMS Project Officer. All patches shall be recorded in the appropriate system documentation on an ongoing basis. Please refer to deliverable schedule for more details.

The Contractor shall perform backups of the local (either Rockville or Las Vegas) servers and systems following procedures documented in the DDMS Backup and Recovery Plan.

The Contractor shall compile two (2) activity reports per month. One shall be due mid-month and one at month-end. Each shall detail the month's activity to-date. These reports shall include a detailed description of any major maintenance, software updates, or configuration changes. The reports shall also include descriptive information on each trouble call or any system malfunction, including resolution of the problem and the time period it took to clear the event. In addition, these reports shall include monthly performance statistics (i.e., approximately how much vendor labor time was used for each task area or trouble call, number of running hours, number of downtime hours, etc.).

The Contractor shall perform database recovery, system restore/rebuild, operating system reinstall, and equipment reboots/restarts as needed to resolve system problems encountered during hearing days as approved/directed by the NRC DDMS Project Officer. The Contractor shall track the occurrence of these types of events and provide, as part of the month-end activity report, a detailed analysis of each event that includes the cause of the event, the resolution of the event, and the labor effort expended to resolve the event.

The Contractor shall coordinate warranty replacement and maintenance for hardware components with the designated warrantor (i.e., Cisco Systems, Dell Computer Corporation) as necessary and applicable, as approved/directed by the NRC DDMS Project Officer following the procedures in the DDMS Configuration Management Plan.

Following the procedures in the DDMS Configuration Management Plan, for all modifications made to DDMS hardware, operating systems, and equipment configurations, the Contractor shall document the modifications, via appropriate updates, system documentation, inventory

Digital Data Management System Operations and Maintenance Statement of Work

records, including the Software Engineering Notebook, Users Guides, operations guides, and inventory databases, as maintenance requests are completed. This will be completed in conjunction with any application or A/V changes made at either location. Documentation updates on the application or the A/V system changes will be completed within thirty (30) calendar days by the Contractor, and the Contractor is responsible for updating the operations guides in all locations.

The Contractor shall be responsible for preparing and submitting to the NRC any software toolkit requests for any new software product, or new software version, that is added to the baseline configuration. It is estimated that this may occur once or twice a year.

The Contractor shall utilize government-furnished equipment listed in Attachment I as emergency replacement components. Further, on a yearly basis on the first business of July, the Contractor shall recommend to the government components that should be purchased by the government to be used as emergency replacements of key existing DDMS components that are not fully redundant or fault tolerant.

The Contractor shall, upon request, produce ad-hoc reports and queries from any DDMS application component system. The NRC estimates that this will require one (1) simple report (e.g., consisting of a query utilizing three or less data sources) and one (1) complex report (e.g., consisting of a query utilizing more than three data sources) per month.

The Contractor shall respond to approximately one (1) or two (2) questions per week from DDMS account holders pertaining to use and technical aspects of the various application systems as directed by the NRC DDMS Project Officer.

The Contractor shall inform the DDMS Project Management Team via the DDMSwebmaster@nrc.gov e-mail account using the internal NRC e-mail system upon completion of each maintenance and operational support activity. The e-mail will define the action taken and identify any subsequent actions that may be necessary.

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

5.1.2 Objectives

5.1.3 Initiation of Work

The Contractor shall have responsibility for, and is authorized without prior specific approval by the NRC DDMS Project Officer to undertake, any necessary actions regarding the items specifically identified in section 5.1.1 so long as the effort takes no more than sixteen (16) hours. The Contractor shall notify the DDMS Project Management Team upon completion of each activity. Notification shall include identification of any issues and/or problems encountered and a brief summary of the resolution.

Digital Data Management System Operations and Maintenance Statement of Work

For items specifically identified in section 5.1.1 that the Contractor determines will take more than 16 hours to complete, the Contractor shall request approval from the NRC DDMS Project Officer before commencing work.

For all other work not specifically identified in section 5.1.1, the NRC DDMS Project Officer shall submit work requests by e-mail or other written correspondence to the Contractor as detailed in section 5.1.4 below. The Contractor shall respond to the work request by e-mail or other written communication to the DDMS Project Management Team within one (1) week of the request. The response shall include the estimated level of effort to complete the activity and supporting detail as requested. The NRC DDMS Project Officer will review the response from the Contractor and will provide further direction to the Contractor within five (5) days of receiving the response.

Application system failures or other critical problems (i.e., Norton Antivirus, backup software, intrusion detection) that require emergency maintenance action on the DDMS discovered during Contractor monitoring efforts shall be remedied immediately. The problem and corrective solution shall be brought to the attention of the DDMS Project Management Team within two (2) hours.

5.1.4 Work Actions Requiring Pre-Approval

Within one (1) week of a work request, the Contractor shall develop and deliver via e-mail to NRC's DDMS Project Management Team, work estimates, schedules and plans for the requested work. NRC's DDMS Project Management Team will review the Contractor's assessment and the NRC DDMS Project Officer will provide comments within two (2) working days of receipt of the Contractor's proposed work plan. The Contractor shall not commence code or data changes without an e-mail authorization from the NRC DDMS Project Officer. Authorized actions shall be performed by the Contractor within five (5) working days of authorization, unless a longer time is approved by the NRC DDMS Project Officer.

5.1.5 Standard Work Approach

DDMS system maintenance requests will routinely involve software releases of the COTS products that make up the DDMS system. The Contractor shall inform the NRC DDMS Project Officer when releases to underlying COTS products are available and request that the Project Officer submit a change request to the DDMS Change Control Board.

No changes shall be made to the application source code without written authorization from the NRC DDMS Project Officer. Once that authorization is provided, changes shall be made in accord with the DDMS Configuration Management Plan. It is the responsibility of both NRC DDMS Project Officer and the Contractor to ensure that the introduction of any new product to the application system is consistent with the authorized list of vendor products (a.k.a., the toolkit) approved by NRC's Environmental Change Control Board.

The Contractor shall maintain a current copy of the DDMS production system in a near production configured test and development environment and any other NRC owned and operated computing installation. The Contractor shall adhere to the testing procedures defined in the DDMS Configuration Management Plan to ensure continued compatibility with existing NRC applications.

Digital Data Management System
Operations and Maintenance Statement of Work

5.1.6 Specialized Maintenance Support

The Contractor shall provide access to vendor system specialists to support key software and hardware components as needed to troubleshoot unique or atypical technical situations, such as the courtroom evidence presentation system, portal technologies, and multi-media recording technologies. It is estimated that each of these products may experience one (1) problem per year requiring sixty (60) hours of specialized expertise that will be employed in conjunction with Contractor's regular O&M staff.

5.1.7 Scheduled Deliverables

Individual deliverables and specific due dates shall be negotiated with each planned maintenance release and in accord with directions from the NRC DDMS Project Officer. The Contractor shall deliver to the DDMS Project Management Team, via the DDMSwebmaster@nrc.gov e-mail account using the internal NRC e-mail system, both draft and final versions of all new and updated documentation deliverables associated with each maintenance or operations support activity. Drafts shall be delivered for NRC review in time to provide a sufficient period for NRC review (three (3) to five (5) working days). Final versions shall be delivered incorporating comments and/or changes provided to the NRC DDMS Project Officer.

The Contractor shall deliver all required reports and any correspondence to the DDMS Project Management Team via the DDMSwebmaster@nrc.gov e-mail account using the internal NRC e-mail system.

Related SOW section/ task	Deliverable Name	Delivery Schedule
Section 5.1.1.1 Paragraph 3	Report of software or hardware licenses or maintenance agreements	First business day of each quarter
Section 5.1.1.1 Paragraph 6	Training activity report	First business day of each quarter
Section 5.1.1.2 Paragraph 1	Verify EHD documents have been indexed into DDMS	Daily (Working Days)
Section 5.1.1.2 Paragraph 2	Verify DDMS ad hoc documents are available in ADAMS	Daily (Working Days)
Section 5.1.1.2 Paragraph 3	Verify Environmental Status	Daily (Working Days)
Section 5.1.1.2 Paragraph 4	Verify data backups	Daily (Working Days)
Section 5.1.1.2 Paragraph 5	Verify remote site connectivity	Daily (Working Days)
Section 5.1.1.2 Paragraph 6	Verify Data and File Replication	Daily (Working Days)
Section 5.1.1.3 Paragraph 1	System Diagnostic Tests Report	Weekly
Section 5.1.1.4	Patch Installation Report	Weekly

Digital Data Management System
Operations and Maintenance Statement of Work

Paragraph 2 Section 5.1.1.4 Paragraph 4 Section 5.1.1.4 Paragraph 5 Section 5.1.1.4 Paragraph 7	Mid-month activity report End of month activity report Updates to documentation as a result of hardware, operation system, or component configuration change	Delivery one (1) working day prior to scheduled meeting Delivery one (1) working day prior to scheduled meeting Appropriate documentation update within thirty (30) calendar days of configuration change
Section 5.1.1.4 Paragraph 9	Recommendation for on hand emergency replacement equipment	Once a year on the first business day of July

5.2 Task Two – IT Related Security Activities

5.1.2 Objectives

The primary objective of this task is to ensure that the DDMS remains available for use throughout its entire life-cycle and meets applicable Federal and Agency IT security requirements. Security measures that are monitored, tested, and updated are crucial to the availability of the DDMS. Additionally, Federal IT systems are governed by federal statutes, laws, and standards. Strict adherence to the rules and regulations are a must for Federal IT systems to remain in production. This Task is specifically designed to maintain a strong security posture that is in alignment with Federal IT systems rules and regulations.

5.2.2 Scope of Security Activity

The Contractor shall ensure that DDMS maintains a security posture commensurate with FIPS 200 “Minimum Security Requirements for Federal Information and Information Systems” for Moderate¹⁰ systems, the Moderate control baseline from NIST SP 800-53 “Recommended Security Controls for Federal Information Systems”, and all applicable provisions in MD 12.5 “Automated Information Security Program”.

The Contractor shall be responsible for reviewing security logs on a daily basis using automated analysis tools for the DDMS routers, firewalls, servers, and workstations to ensure the continued availability of the DDMS using government-furnished equipment and resources where appropriate. The Contractor shall deliver a weekly report detailing the results of the daily security reviews to the DDMS Project Management Team.

The Contractor, on a calendar year based quarterly cycle, shall evaluate the security posture of the DDMS by conducting a test of twenty-five (25) percent of the current in-place NIST SP 800-53, Recommended Security Controls for Federal Information Systems and FIPS 200 Minimum Security Requirements for Federal Information and Information Systems. The Contractor shall evaluate the security controls that are required for the DDMS using Contractor resources that are not directly under the supervision of the Contractor division or department that provides

¹⁰ The level of controls needed to meet these requirements is based on the level of information sensitivity as determined by the DDMS Security Categorization Document. The Information Sensitivity level of the DDMS is categorized as moderate.

Digital Data Management System Operations and Maintenance Statement of Work

operations and maintenance support. The controls shall be selected by the NRC DDMS Project Officer and provided to the Contractor ten (10) calendar days prior to the required evaluation date. The process for conducting the evaluation will be completed by the Contractor within twenty-five (25) calendar days of receiving the selected controls using the current version of NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. Upon completing the evaluation, the Contractor shall provide the NRC DDMS Project Officer a report detailing the findings of the evaluation and a Plan of Action for resolving any issues found during the evaluation. The report and plan of action shall be delivered no more than five (5) working days after the completion of the evaluation. The evaluation conducted during the second quarter of the calendar year shall take place at the NRC Las Vegas hearing facility.

In conducting all DDMS IT security functions, the Contractor shall follow appropriate NRC IT security policy, procedures, and standards as defined on the NRC CSO website and DDMS specific IT Security Procedures, as defined in the DDMS Security Guidelines document.

The Contractor shall be responsible for providing a plan of action to the DDMS Project Team that ensures the DDMS software and hardware components adhere to the latest version of all applicable Federal Information Technology Security guidance and standards. Guidance and standards include, but is not limited to, NRC Management Directive 12.5 Automated Information Security Program, and the National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS and Committee on National Security Systems (CNSS) policy, directives, instructions and guidance.

On a yearly basis, the Contractor shall provide qualified staff to meet with OIS Staff, CSO Staff, other NRC Contractors, and the DDMS Project Management Team to assist in efforts to complete IT security activities including:

- Security Risk Assessment - The Contractor shall work with the NRC DDMS Project Officer in performing Risk Assessment activities according to NRC policy, standards, and guidance. The Contractor shall perform Risk Assessment activities that include analyzing how the architecture implements the NRC documented security policy for the system and 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.
- System Security Plan - The Contractor shall assist in maintaining 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 shall ensure that all controls required to be implemented are documented in the SSP.
- Security Test & Evaluation (ST&E) - The Contractor shall support ST&E activities, including, but not limited to, coordinating the ST&E and developing the ST&E Plan and executing ST&E test cases and documenting test results.
- Plan of Action and Milestones (POA&M) Maintenance & Reporting - The Contractor shall assist in the development and implementation of solutions that provide a means of planning and monitoring corrective actions.

Digital Data Management System Operations and Maintenance Statement of Work

- Certification and Accreditation Documentation - The Contractor shall assist in the creation, updating, and maintenance of all Certification and Accreditation (C&A) documentation as directed by the NRC DDMS Project Officer. Deliverables may include, but are not limited to the following items: Privacy Impact Assessment, System Security Categorization, Risk Assessment Report, System Security Plan, Memorandum of Understanding, Interconnection Security Agreement, ST&E Plan, Security Assessment Report, Vulnerability Assessment Report, POA&M, Deviation Request, and Business Impact Analysis and Contingency Plan.

On a yearly basis, DDMS IT Security Documentation shall be independently reviewed and tested by an Agency-provided Contractor or by the DDMS Project Team. The Contractor shall use the results of these tests as a basis for updating the documents listed in the DDMS Table of Documents document. Additionally, the Contractor shall be fully responsive and provide all needed support in circumstances in which the DDMS Project Management Team members independently inspect and test security components.

The Contractor, on a quarterly basis, shall evaluate the results of a comprehensive security scan of the DDMS by the DDMS Project Team using the OIS approved security scanning tool set. Upon completion of the scans, the Contractor shall be provided the full results of the scans and shall resolve or mitigate: (1) categorized critical issues within thirty (30) calendar days of receiving the scan results; (2) categorized high issues within forty-five (45) calendar days of receiving the scan results; (3) categorized medium issues within sixty (60) calendar days of receiving the scan results; and (4) categorized low issues within seventy-five (75) calendar days of receiving the scan results. The Contractor shall provide the DDMS Project Management Team with weekly updates regarding the progress of the resolution or mitigation of the scan results.

On a yearly basis in the April/May timeframe, at the direction of the NRC DDMS Project Officer, the Contractor shall exercise the DDMS Contingency Plan. The Contingency Plan test may take the form of a full-blown contingency test or a table-top exercise and should take no more than ten (10) calendar days to complete. At a minimum, a full Contingency Plan test will occur every three years. Within ten (10) working days of the conclusion of the Contingency Plan test, the Contractor shall conduct a lessons learned session of no more than one (1) hour, during which it shall provide the DDMS Project Team with a detailed report on the results of the test, and document the Contingency Plan test results in an NRC-approved format. The DDMS Contingency Plan shall be updated by the Contractor within ten (10) working days after the lessons learned session is held.

On a quarterly basis, at the direction of the DDMS Project team, the Contractor shall test the DDMS incident response capabilities as defined in the DDMS Incident Response Plan. Within ten (10) working days of the conclusion of the incident response test, the Contractor shall conduct a lessons learned session of no more than one (1) hour, during which it shall provide the DDMS Project Team with a detailed report on the results of the test, and document the incident response test results in an NRC-approved format. The DDMS Incident Response Plan shall be updated by the Contractor within ten (10) working days after the lessons learned session is held.

On a quarterly basis, the Contractor shall test recovery of data from backup tapes following the test procedures outline in the DDMS Backup and Recovery Plan. Within five (5) working days of the conclusion of the data recovery test, the Contractor shall conduct a lessons learned

Digital Data Management System
Operations and Maintenance Statement of Work

session of no more than one (1) hour, during which it shall provide the DDMS Project Team with a detailed report on the results of the test, and document the data recovery test results in a NRC approved format. As needed based on the results of the data recovery exercise, the DDMS Backup and Recovery Plan shall be updated within ten (10) of the delivery of the data recovery test report.

5.2.3 Initiation of Work

Unless otherwise noted, the Contractor shall have the responsibility to, and is authorized to take, necessary actions for the items specifically identified in section 5.2.2 without prior specific approval by the NRC DDMS Project Officer. The Contractor shall notify the DDMS Project Management Team upon completion of each such activity. Notification shall include identification of any issues and/or problems encountered and a brief summary of the resolution.

If discovered during monitoring efforts conducted by the Contractor in its role of providing operations and production support or by monitoring efforts conducted by NRC Network Operations Center staff or Contractors, potential security vulnerabilities (i.e., Norton Antivirus, intrusion detection) or other critical problems that require emergency maintenance action on DDMS shall immediately be corrected and brought to the attention of the DDMS Project Management Team.

5.2.4 Scheduled Deliverables

Related SOW task or section	Deliverable Name	Delivery Schedule
Section 5.2.2 Paragraph 1	Security Log Review Report	Weekly
Section 5.2.2 Paragraph 2	NIST 800-53 Security Control Review Report	Quarterly – Within five (5) working days of the completion of the NIST SP 800-53 control set evaluation
Section 5.2.2 Paragraph 7	Resolution/Mitigation of Vulnerability Scan Findings	Categorized critical issues within thirty (30) calendar days of receiving the scan results Categorized high issues within forty-five (45) calendar days of receiving the scan results Categorized medium issues within sixty (60) calendar days of receiving the scan results Categorized low issues within seventy-five (75) calendar days of receiving the scan results
Section 5.2.2 Paragraph 8	Yearly Contingency Plan Test Results	Yearly - within ten (10) working days of test completion

Digital Data Management System
Operations and Maintenance Statement of Work

Section 5.2.2 Paragraph 8	Contingency Plan Test Lessons Learned Presentation and Detailed Results	Yearly - within ten (10) working days of test completion
Section 5.2.2 Paragraph 8	Updated Contingency Plan	Yearly - within ten (10) working days of lessons learned presentation
Section 5.2.2 Paragraph 9	Quarterly Incident Response Test Results	Quarterly - within ten (10) working days of test completion
Section 5.2.2 Paragraph 9	Incident Response Test Lessons Learned Presentation and Detailed Results	Quarterly - within ten (10) working days of test completion
Section 5.2.2 Paragraph 9	Updated Incident Response Plan	Quarterly - within ten (10) working days of lessons learned presentation
Section 5.2.2 Paragraph 10	Quarterly Data Recovery Test Results	Quarterly - within five (5) working days of test completion
Section 5.2.2 Paragraph 10	Data Recovery Test Lessons Learned Presentation and Detailed Results	Quarterly - within five (5) working days of test completion
Section 5.2.2 Paragraph 10	Updated Backup and Recovery Plan	Quarterly - within ten (10) working days of lessons learned presentation

5.3 Task Three – Hearing/Meeting Support

5.1.2 Objectives

The purpose of this task is to ensure that the Contractor provides sufficient qualified staffing (e.g., staff capable of supporting the DDMS courtroom evidence presentation system, operating the DDMS application, supporting Clerk of Court functions) to support ASLBP hearings or meetings.

5.3.2 Scope of Hearing/Meeting Support

For hearings held in the ASLBP's Rockville, MD hearing room or its Las Vegas, NV hearing facility, the Contractor shall provide as many as two (2) individuals per site¹¹ to provide operational support for the A/V system and DDMS Application for periods generally not exceeding ten (10) hours per hearing day and generally during the work week. Due to the nature of legal proceedings, however, it may become necessary for operational support to extend beyond the ten (10) hour period as well as during weekends and holidays.

For hearings held at a locations other than the ASLBP's Rockville, MD hearing room or its Las Vegas, NV hearing facility, the Contractor shall provide in Rockville, MD, one (1) individual capable of supporting the technical operation of the DDMS for periods generally not exceeding ten (10) hours per hearing day and generally during the work week. Due to the nature of legal

¹¹ HLW hearings held in Rockville or Las Vegas will typically involve video-conferencing between the two sites. Contractor support is needed in both locations when the hearing is video-conferenced.

Digital Data Management System Operations and Maintenance Statement of Work

proceedings, however, it may become necessary for operational support to extend beyond that ten (10) hour period as well as during weekends and holidays.

The Contractor shall conduct a thorough system test of the A/V system, to include A/V feeds to external distribution services such as videoconferencing units, the ASLBP web streaming contractor, NRC internal cable broadcast, etc., to ensure that the hearing room is ready for that day's hearing/meeting at least one (1) hour prior to the beginning of scheduled hearings/meetings.

The Contractor shall conduct a thorough system test of the DDMS application to ensure that the hearing room is ready for that day's hearing/meeting at least one (1) hour prior to the beginning of scheduled hearings/meetings.

With direction from the NRC DDMS Project Officer, the Contractor shall work with NRC-contracted court reporters, to provide assistance to ensure that the Line 21¹² signals are captured for the purpose of close-captioning and video transcript synchronization.

The Contractor shall assist the ASLBP clerk of the court in performing any session beginning or ending data migration or other activities required to support the day's proceedings.

During hearings held in Rockville, Las Vegas, or other sites in the continental United States, the Contractor shall provide the Panel with one (1) individual for day-to-day operational support for hearing-related activities that include, but are not be limited to, electronically marking exhibits, displaying electronic evidence, and receiving electronic documents from hearing participants and adding those documents to DDMS as ad hoc documents or exhibits. Hearings will generally not exceed ten (10) hours per hearing day and are generally held during the work week. Due to the nature of legal proceedings, however, it may become necessary for operational support to extend beyond that ten (10) hour period as well as during weekends and holidays.

The Contractor shall provide operational support on the A/V subsystem to the clerk of court and/or participants involved in hearings/meetings utilizing the DDMS system.

On an as needed basis, but no more than once per month, the Contractor shall provide input into lessons learned briefings based on their experience supporting hearings and/or meetings.

5.3.3 Initiation of Work

In general, the NRC DDMS Project Officer will notify the Contractor by e-mail at least two (2) weeks before any scheduled hearing/meeting indicating the level of support needed. Nonetheless, due to the nature of legal/regulatory proceedings, the Contractor should expect that, on occasion, there may be as little as twenty-four (24) hours notice from the NRC DDMS Project Officer requesting hearing/meeting support.

¹² Line 21 is the industry-standard track of a video signal used by closed-captioning systems to embed the text onto the video signal. The serial output of the transcription machine is connected to a Line 21 encoder. The Court Reporter/closed captionist will connect his/her stenographic machine to a DDMS workstation running the Total Eclipse Court Reporting/Closed Caption software. This workstation and software will translate the output from the stenographic machine and provide input to the closed caption encoder that provides the text for the real-time transcript as well as the closed caption text displayed on the hearing room monitors to assist the hearing impaired.

Digital Data Management System
Operations and Maintenance Statement of Work

The Contractor shall continue to support scheduled hearings/meetings that exceed the planned daily ten (10) hour duration without requiring prior approval from the NRC DDMS Project Officer. If an ASLBP presiding officer directs that a particular hearing session shall continue beyond the planned schedule, the Contractor shall consider the assignment extended and should notify the NRC DDMS Project Officer regarding the session extension.

5.3.4 Scheduled Deliverables

Related SOW task / section	Deliverable Name	Delivery Schedule
Section 5.3.2 Paragraph 4	Audio visual system check	Daily per hearing day

5.4 Task Four – Application Enhancements, Development and Test Environment

5.1.2 Objectives

The objective of this task is to provide operational flexibility for the DDMS as policies and procedures within the NRC, ASLBP, and the industry evolve. This task both enables DDMS enhancements and provides for specific procedures to control how those enhancements are introduced, evaluated, and implemented.

The NRC has two (2) test environments that are used in conjunction with the deployment of new systems and modifications to others.

The first is the CTF, which is operated independent of the NRC's production environment. The CTF provides a flexible environment to facilitate the various types of standard system life cycle testing. Any systems that are deployed in the agency's production environment must complete an Acceptance Test that involves verifying security and operational compliance, as well as overall compatibility, with the production environment. Also, some COTS and/or desktop deployments new to the production environment may require a Desktop Acceptance Test.

The second test environment is the TAE, which is used to perform impact analysis and quality assurance on system changes, upgrades, and refinements before they are migrated to the production environment, as prescribed by the NRC's PMM.

5.4.2 Scope of Application Enhancements Activity

The Contractor shall have available qualified staff capable of making enhancements to the DDMS based upon requests from the NRC DDMS Project Officer for changes that have been approved by the DDMS CCB. The Contractor shall provide a requirements document and implementation approach for each CCB requested change or group of changes for approval by the NRC DDMS Project Officer. This document shall include an estimate of the amount of effort required to complete the development, testing, implementation, documentation updates, and potential IT security impacts associated with the requested change.

The Contractor shall use a government-furnished development system to develop and test changes that may be installed at the Contractor's facility, provided the facility has been accredited by NRC for processing information at the moderate sensitivity level. Although the

Digital Data Management System Operations and Maintenance Statement of Work

DDMS may process sensitive unclassified non-safeguards information, the Contractor shall only use publicly available data for testing purposes.

Once the enhancement or change is completed, the Contractor shall follow the procedures detailed in the DDMS Configuration Management Plan for testing and deployment into the production environment.

Within ten (10) working days after deployment, the Contractor shall ensure that the DDMS installation into the CTF, the TAE, and any other DDMS installation owned and operated by the NRC are updated with the new code baseline as well as the Rational code base repository as defined by PMM procedures.

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

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

All development and test systems shall be protected based on FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems for Moderate" systems, the Moderate control baseline from NIST SP 800-53 "Recommended Security Controls for Federal Information Systems", and all applicable provisions in MD 12.5 "Automated Information Security Program".

Development and test systems shall be physically and/or logically separated from each other and shall not be connected to the NRC production environment.

5.4.3 Scope of Test Environment Activity

The Contractor shall maintain the two (2) above-identified working test environments. The first shall be located in the CTF and shall consist of a government-furnished computer configured to allow connections from other NRC systems that send/pull data to/from the DDMS.

The Contractor shall also maintain a second system in the NRC's TAE environment. This system only needs to include components that are required to simulate the external interface connections to in-house NRC systems.

Additionally, the Contractor shall maintain a government-furnished test system at their location that replicates the DDMS as closely to the installed system as possible, including a simulated WAN connection, clustered server environment, and non-clustered video encoding equipment. The Contractor facility and specific location where the test system will reside must meet both Federal and NRC information system security requirements as well as physical security requirements. The level of controls needed to meet these requirements is based on the level of information sensitivity determined by the DDMS Security Categorization Document, which currently is categorized as moderate. Although the DDMS may process sensitive unclassified non-safeguards information, the Contractor shall only use publicly available data for testing purposes.

Digital Data Management System Operations and Maintenance Statement of Work

The Contractor shall ensure that the CTF and TAE maintain the current operating version of the DDMS application.

Within six months of Contract award, the NRC shall provide updated components to replace aging development and test system components. The Contractor shall configure and integrate those updated components into the appropriate environment strictly adhering to configuration management procedures outlined in the DDMS Configuration Management Plan.

5.4.4 Initiation of Work

The NRC DDMS Project Officer shall send a request to the Contractor to initiate any enhancement as defined in section 5.4.2. The NRC DDMS Project Officer shall send the Contractor the DDMS CCB approval form and detailed information regarding the requested enhancement.

The Contractor shall have authority to take necessary actions for each item listed in section 5.4.3 without prior approval. The Contractor shall notify the NRC DDMS Project Officer upon completion of each activity. Notification shall include identification of any issues and/or problems encountered and a brief summary of the resolution.

5.4.5 Scheduled Deliverables

Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.4.2 Paragraph 1	Change Proposal Implementation Plan	As defined in the DDMS Configuration Management Plan
Section 5.4.2 Paragraph 3	Requested Enhancement	As detailed in approved implementation plan
Section 5.4.2 Paragraph 4	Code Baseline deployed to all DDMS installations	Within Ten (10) working days of deployment to production
Section 5.4.2 Paragraph 4	Rational Code Base Repository	Within Ten (10) working days of deployment to production

5.5 Task Five – Training

5.5.1 Objectives

The objective of this task is to establish a flexible training program to address the needs of a widely disbursed user community by leveraging existing technology where possible.

5.5.2 Scope of Training Activity

The Contractor shall propose a training approach as well as develop training and course material, consistent with the DDMS Training Plan, that leverages existing technology where possible and provides the greatest exposure to a user community that:

1. Is widely disbursed;

**Digital Data Management System
Operations and Maintenance Statement of Work**

2. Has varying levels of computer skills;
3. May or may not have access to high speed internet services;
4. Has limited time or resources to attend training; and
5. Will require periodic re-training.

In conjunction with any system enhancement developed and implemented as part of task four of this contract, the Contractor shall update all system documentation, training material, and DDMS context help within twenty (20) working days to reflect the implemented enhancement.

The Contractor shall provide all training material to the NRC DDMS Project Officer for review and approval before making it available to the user community.

Each month, the Contractor shall provide two (2) three (3)-hour training sessions for up to twenty (20) individuals. Locations shall alternate between the Rockville and Las Vegas facilities each month. The Contractor shall design an approach to conducting training that utilizes DDMS functionality where possible (i.e., video conferencing, portal-based training, etc.).

5.5.3 Initiation of Work

At least fourteen (14) calendar days prior to the scheduled training date, the NRC DDMS Project Officer shall send a notification to the Contractor indicating the date, time, and subject of training to be conducted within a given month.

The Contractor shall have the authority to begin updating training material once the NRC has fully tested and accepted any system enhancement.

5.5.4 Scheduled Deliverables

Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.5.2 Paragraph 2	Update to training material based on approved enhancement	Within twenty (20) working days of implemented enhancement
Section 5.5.2 Paragraph 4	Two (2), three (3)-hour training sessions per month, one (1) each in the Rockville and Las Vegas hearing facilities	On Scheduled Date

5.6 Optional Tasks

5.6.1 Optional Task 6A - Technology Refresh of Rockville Data Processing Sub-System

5.6.1.1 Optional Task 6A - Objective

The objective of this task is to provide a vehicle in which the hardware components of the DDMS installed in Rockville can keep pace with the current state of technology. Hardware

Digital Data Management System Operations and Maintenance Statement of Work

technology changes at a rapid pace and typically has a fixed lifetime for warranty service and product support. Therefore, to maintain the reliability and performance of the DDMS, provisions need to be in place to adapt to the changing IT environments and support structures.

5.6.1.2 Optional Task 6A Scope

Following configuration management procedures outlined in the DDMS Configuration Management Plan, the Contractor shall replace the Rockville Data Processing components identified as RKDPSS in the revised Attachment II Sub-System Component column, that are chosen by the DDMS Project Management Team at the time of task execution with comparable hardware provided by the government that meets or exceeds current technical specifications. The operating systems of any new servers and workstations shall be on the approved Agency operating system list at the time this task is executed.

The Contractor shall provide the NRC with a detailed technology refresh plan that adheres to all NRC policies regarding the introduction of new hardware and/or software components into the NRC's IT infrastructure and at a minimum includes a components list, integration plan, migration plan, and any other Project Management Methodology (PMM) documentation appropriate for the type of technology refresh that is recommended. Additionally, the detailed technology refresh plan shall include a schedule for the delivery of documentation updates related to any Security Certification and Accreditation Activities required for the new or updated components to be integrated into the NRC production environment. This includes updates to all required PMM documents including, but not limited to, the DDMS Security Categorization, the DDMS Risk Assessment, the DDMS Security Plan, the DDMS Contingency Plan, the DDMS Security Test and Evaluation Plan, the DDMS Interface Control Document, and the DDMS Operational Support Guide.

The technology refresh plan should be structured so as not to interfere with or hamper any ongoing proceedings that are being conducted. The technology refresh plan shall be delivered within thirty (30) calendar days of the execution of this optional task.

Upon approval of the technology refresh plan, the Contractor shall implement the technology refresh based upon the approved components list and the integration and migration plans, and shall complete the refresh within one hundred eighty (180) calendar days of receiving approval to proceed.

The Contractor shall leverage existing software maintenance licenses when possible.

5.6.1.3 5.6.1.3 Optional Task 6A Initiation of Work

If the NRC determines that a technology refresh of the Rockville data processing components is warranted, the government will exercise optional task 6A. When the task is exercised, a list of components to be refreshed and provided by the government will be attached to the notification. It should be noted that not all components associated with a given sub-task may be included in the selected component list. Upon the Contractor's acceptance of the Contract modification, the Contractor shall begin developing the technology refresh plan and shall deliver it to the DDMS Project Management Team within thirty (30) calendar days of Contractor acceptance.

The DDMS Project Management Team will evaluate the technology refresh proposal and

Digital Data Management System Operations and Maintenance Statement of Work

present a recommendation to ASLBP Management for its consideration, along with a request for a Go/No Go decision. The Contractor will be notified by the NRC DDMS Project Officer within ten (10) working days of the receipt of the refresh plan of the ASLBP Management decision. If a Go decision is issued, the Contractor shall begin work immediately on the technology refresh according to the technology refresh proposal. Should a No Go decision be issued, the Contractor shall terminate any activity related to this task.

The estimated early start for sub-task 6A would be October 2013.

See deliverable list in section 5.7.

5.6.2 Optional Task 6B - Technology Refresh of Las Vegas Data Processing Sub-System

5.6.2.1 Optional Task 6B - Objective

The objective of this task is to provide a vehicle in which the hardware components of the DDMS installed in Las Vegas can keep pace with the current state of technology. Hardware technology changes at a rapid pace and typically has a fixed lifetime for warranty service and product support. Therefore, to maintain the reliability and performance of the DDMS, provisions need to be in place to adapt to the changing IT environments and support structures.

5.6.2.2 Optional Task 6B Scope

Following configuration management procedures outlined in the DDMS Configuration Management Plan, the Contractor shall replace the Las Vegas Data Processing components identified as LVDPSS in the revised Attachment II Sub-System Component column, that are chosen by the DDMS Project Management Team at the time of task execution with comparable hardware provided by the government that meets or exceeds current technical specifications. The operating systems of any new servers and workstations shall be on the approved Agency operating system list at the time this task is executed.

The Contractor shall provide the NRC with a detailed technology refresh plan that adheres to all NRC policies regarding the introduction of new hardware and/or software components into the NRC's IT infrastructure and at a minimum includes a components list, integration plan, migration plan, and any other Project Management Methodology (PMM) documentation appropriate for the type of technology refresh that is recommended. Additionally, the detailed technology refresh plan shall include a schedule for the delivery of documentation updates related to any Security Certification and Accreditation Activities required for the new or updated components to be integrated into the NRC production environment. This includes updates to all required PMM documents including, but not limited to, the DDMS Security Categorization, the DDMS Risk Assessment, the DDMS Security Plan, the DDMS Contingency Plan, the DDMS Security Test and Evaluation Plan, the DDMS Interface Control Document, and the DDMS Operational Support Guide.

Upon approval of the technology refresh plan, the Contractor shall implement the technology refresh based upon the approved components list, and the integration and migration plans, and shall complete the refresh within one hundred eighty (180) calendar days of receiving approval to proceed.

Digital Data Management System Operations and Maintenance Statement of Work

The Contractor shall leverage existing software maintenance licenses when possible.

5.6.2.3 5.6.2.3 Optional Task 6B Initiation of Work

If the government determines that a technology refresh of the Las Vegas data processing components is warranted, the government will exercise optional task 6B. When the task is exercised, a list of components to be refreshed and provided by the government will be attached to the notification. It should be noted that not all components associated with a given sub-task may be included in the selected component list. Upon the Contractor's acceptance of the Contract modification, the Contractor shall begin the development of the technology refresh plan and deliver it to the DDMS Project Management Team within thirty (30) calendar days of Contractor acceptance.

The DDMS Project Management Team will evaluate the technology refresh proposal and present a recommendation to ASLBP Management for its consideration, along with a request for a Go/No Go decision. The Contractor will be notified by the NRC DDMS Project Officer within ten (10) working days of the receipt of the refresh plan of the ASLBP Management decision. If a Go decision is issued, the Contractor shall begin work immediately on the technology refresh according to the technology refresh proposal. Should a No Go decision be issued, the Contractor shall terminate any activity related to this task.

The estimated early start for sub-task 6B would be October 2014.

See deliverable list in section 5.7.

5.6.3 Optional Task 6C - Technology Refresh of Rockville Audio/Visual Sub-System

5.6.3.1 Optional Task 6C - Objective

The objective of this task is to provide a vehicle in which the audio/visual components of the DDMS installed in Rockville can continue to provide quality audio visual service. Audio video technology changes at a rapid pace and typically has a fixed lifetime for warranty service and product support. Therefore, to maintain the reliability and performance of the DDMS, provisions need to be in place to adapt to the changing audio video environments and support structures.

5.6.3.2 Optional Task 6C Scope

Following configuration management procedures outlined in the DDMS Configuration Management Plan, the Contractor shall replace the Rockville Audio Visual Sub-System components, identified as RKAVSS in the revised Attachment II Sub-System Component column, that are chosen by the DDMS Project Team at the time of task execution with comparable components provided by the government that meets or exceeds current technical specifications and maintain existing functionality.

The Contractor shall provide the NRC with a detailed technology refresh plan that adheres to all NRC policies regarding the introduction of new hardware and/or software components into the NRC's IT infrastructure and at a minimum includes a components list, integration plan, migration plan, and any other Project Management Methodology (PMM) documentation appropriate for the type of technology refresh that is recommended. Additionally, the detailed technology refresh plan shall include a schedule for the delivery of documentation updates related to any

Digital Data Management System Operations and Maintenance Statement of Work

Security Certification and Accreditation Activities required for the new or updated components to be integrated into the NRC production environment. This includes updates to all required PMM documents including, but not limited to, the DDMS Security Categorization, the DDMS Risk Assessment, the DDMS Security Plan, the DDMS Contingency Plan, the DDMS Security Test and Evaluation Plan, the DDMS Interface Control Document, and the DDMS Operational Support Guide.

Upon approval of the technology refresh plan, the Contractor shall implement the technology refresh based upon the approved components list, and the integration and migration plans, and shall complete the refresh within one hundred eighty (180) calendar days of receiving approval to proceed.

The design shall utilize high definition video components when possible.

The design shall utilize existing cabling when possible. In instances when existing cable is not sufficient, the Contractor shall provide cabling requirements to the government for its review. Should the government accept the proposed cabling requirements; the Government will furnish necessary cabling in the Rockville Hearing room.

The design shall include the same number of inputs and outputs that exist at the time this task is executed.

The Contractor shall leverage existing software maintenance licenses when possible.

The estimated early start for sub-task 6C would be October 2013.

5.6.3.3 5.6.3.3 Optional Task 6C Initiation of Work

If the government determines that a technology refresh of the Rockville audio video components is warranted, the government will exercise optional task 6C. When the task is exercised, a list of components to be refreshed and provided by the government will be attached to the notification. It should be noted that not all components associated with a given sub-task may be included in the selected component list. Upon the Contractors acceptance of the Contract modification, the Contractor shall begin the development of the technology refresh plan and deliver it to the DDMS Project Team within thirty (30) calendar days of Contractor acceptance.

The DDMS Project Management Team will evaluate the technology refresh proposal and present a recommendation to ASLBP Management for its consideration, along with a request for a Go/No Go decision. The Contractor will be notified by the NRC DDMS Project Officer within ten (10) working days of the receipt of the refresh plan of the ASLBP Management decision. If a Go decision is issued, the Contractor shall begin work immediately on the technology refresh according to the technology refresh proposal. Should a No Go decision be issued, the Contractor shall terminate any activity related to this task.

The estimated early start for sub-task 6C would be October 2013.

See deliverable list in section 5.7.

Digital Data Management System
Operations and Maintenance Statement of Work

5.6.4 Optional Task 6D - Technology Refresh of Las Vegas Audio Visual Sub-System

5.6.4.1 Optional Task 6D - Objective

The objective of this task is to provide a vehicle in which the audiovisual components of the DDMS installed in Las Vegas can continue to provide quality audio visual service. Audio video technology changes at a rapid pace and typically has a fixed lifetime for warranty service and product support. Therefore, to maintain the reliability and performance of the DDMS, provisions need to be in place to adapt to the changing audio video environments and support structures.

5.6.4.2 Optional Task 6D Scope

Following configuration management procedures outlined in the DDMS Configuration Management Plan, the Contractor shall replace the Las Vegas Audio Visual Sub-System components, identified as LVAVSS in the revised Attachment II Sub-System Component column, that are chosen by the DDMS Project Team at the time of task execution with comparable components provided by the government that meets or exceeds current technical specifications and maintain existing functionality.

The Contractor shall provide the NRC with a detailed technology refresh plan that adheres to all NRC policies regarding the introduction of new hardware and/or software components into the NRC's IT infrastructure and at a minimum includes a components list, integration plan, migration plan, and any other Project Management Methodology (PMM) documentation appropriate for the type of technology refresh that is recommended. Additionally, the detailed technology refresh plan shall include a schedule for the delivery of documentation updates related to any Security Certification and Accreditation Activities required for the new or updated components to be integrated into the NRC production environment. This includes updates to all required PMM documents including, but not limited to, the DDMS Security Categorization, the DDMS Risk Assessment, the DDMS Security Plan, the DDMS Contingency Plan, the DDMS Security Test and Evaluation Plan, the DDMS Interface Control Document, and the DDMS Operational Support Guide.

Upon approval of the technology refresh plan, the Contractor shall implement the technology refresh based upon the approved components list, and the integration and migration plans, and shall complete the refresh within one hundred eighty (180) calendar days of receiving approval to proceed.

The design shall utilize high definition video components when possible.

The design shall utilize existing cabling when possible. In instances when existing cabling is not sufficient, the Contractor shall provide cabling requirements to the government for its review. Should the government accept the proposed cabling requirements, the Contractor shall furnish necessary cabling in the Las Vegas Hearing facility.

The design shall include the same number of inputs and outputs that exist at the time this task is executed.

The Contractor shall leverage existing software maintenance licenses when possible.

Digital Data Management System
Operations and Maintenance Statement of Work

5.6.4.3 5.6.4.3 Optional Task 6D Initiation of Work

If the government determines that a technology refresh of the Las Vegas audio video components is warranted, the government will exercise optional task 6D. When the task is exercised, a list of components to be refreshed and provided by the government will be attached to the notification. It should be noted that not all components associated with a given sub-task may be included in the selected component list. Upon the Contractors acceptance of the Contract modification, the Contractor shall begin the development of the technology refresh plan and deliver it to the DDMS Project Management Team within thirty (30) calendar days of Contractor acceptance.

The DDMS Project Management Team will evaluate the technology refresh proposal and present a recommendation to ASLBP Management for its consideration, along with a request for a Go/No Go decision. The Contractor will be notified by the NRC DDMS Project Officer within ten (10) working days of the receipt of the refresh plan of the ASLBP Management decision. If a Go decision is issued, the Contractor shall begin work immediately on the technology refresh according to the technology refresh proposal. Should a No Go decision be issued, the Contractor shall terminate any activity related to this task.

The estimated early start for sub-task 6D would be October 2014.

See deliverable list in section 5.7.

5.7 Optional Tasks - Estimated Period of Performance and Delivery Schedule

Sub Task 6A - Technology Refresh of Rockville Data Processing Sub-System		
Estimated Task Start:		Earliest Start – October 2013
Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.6.1.2 Paragraph 2	Technology Refresh Plan	Within thirty (30) calendar days of Task Execution
Section 5.6.1.2 Paragraph 2	PMM Documentation	As detailed in the Technology Refresh Plan
Section 5.6.1.2 Paragraph 2	Security Documentation	As detailed in the Technology Refresh Plan
Section 5.6.1.2 Paragraph 3	Implemented Rockville Data Processing Sub-system	No Later than one hundred eighty (180) calendar days after receiving approval of Technology refresh plan
Sub Task 6B - Technology Refresh of Las Vegas Data Processing Sub-System		
Estimated Task Start:		Earliest Start - October 2014

Digital Data Management System
Operations and Maintenance Statement of Work

Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.6.2.2 Paragraph 2	Technology Refresh Plan	Within thirty (30) calendar days of Task Execution
Section 5.6.2.2 Paragraph 2	PMM Documentation	As detailed in the Technology Refresh Plan
Section 5.6.2.2 Paragraph 2	Security Documentation	As detailed in the Technology Refresh Plan
Section 5.6.2.2 Paragraph 3	Implemented Las Vegas Data Processing Sub-System	No Later than one hundred eighty (180) calendar days after receiving approval of Technology refresh plan
Sub Task 6C - Technology Refresh of Rockville Audio Visual Sub-System		
Estimated Task Start:		Earliest Start – October 2013
Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.6.3.2 Paragraph 2	Technology Refresh Plan	Within thirty (30) calendar days of Task Execution
Section 5.6.3.2 Paragraph 2	PMM Documentation	As detailed in the Technology Refresh Plan
Section 5.6.3.2 Paragraph 2	Security Documentation	As detailed in the Technology Refresh Plan
Section 5.6.3.2 Paragraph 3	Implemented Rockville Audio Visual Sub-System	No Later than one hundred eighty (180) calendar days after receiving approval of Technology refresh plan
Sub Task 6D - Technology Refresh of Las Vegas Audio Visual Sub-System		
Estimated Task Start:		Earliest Start - October 2014
Related SOW task / Section	Deliverable Name	Delivery Schedule
Section 5.6.4.2 Paragraph 2	Technology Refresh Plan	Within thirty (30) calendar days of Task Execution
Section 5.6.4.2 Paragraph 2	PMM Documentation	As detailed in the Technology Refresh Plan
Section 5.6.4.2 Paragraph 2	Security Documentation	As detailed in the Technology Refresh Plan

Digital Data Management System
Operations and Maintenance Statement of Work

Section 5.6.4.2 Paragraph 3	Implemented Las Vegas Audio Visual Sub-System	No Later than one hundred eighty (180) calendar days after receiving approval of Technology refresh plan
--------------------------------	---	--

6 Optional Task Seven - Transition Task

6.1 Objective

The objective of the transition task is to provide a knowledge transfer of operating procedures, system design, and system configuration to the successful bidder for any follow-on operations and maintenance support contract. This task also provides a mechanism to transfer hardware components.

6.2 Scope of Transition Task

The Contractor shall make available to the successful bidder individuals in the following roles, each for a period of no more than one hundred sixty-eight (168) hours during the last sixty (60) calendar days of this contract's period of performance:

1. Contractor Project Manager
2. System Administrator
3. Audio Visual Senior Engineer
4. Senior Application Developer
5. Most Senior Day-to-Day operations support individual

The Contractor shall provide a detailed physical configuration diagram of all configured environments installed at their facility.

The Contractor shall disassemble and ready for shipping all government-owned equipment located at their facility to be picked up by a government-provided shipper for delivery to the successful bidder fifteen (15) calendar days prior to last day of this contract.

6.3 Initiation of Work

Should a need arise to transition Contractor support from the incumbent to another entity, the NRC DDMS Project Officer shall send a notification to the Contractor indicating a transition meeting schedule ninety (90) calendar days prior to the last day of the contract's period of performance setting the schedule for meeting the items listed in section 6.2.

7 NRC Computer Security Requirements

The contractors shall only use NRC approved methods to send and receive information considered sensitive.

When e-mail is used, the Contractors 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 the NRC Computer Security Office (CSO).

Digital Data Management System Operations and Maintenance Statement of Work

All Contractor employees, prior to being granted access to NRC computing resources, shall, at a minimum, complete the NRC's Computer Security Awareness Course for General Users and sign the NRC Agency Rules of Behavior for Secure Computer Use.

All work performed at non-NRC facilities shall be conducted in facilities and on IT systems (i.e. servers, workstations, routers, firewalls, etc.) accredited by the NRC using FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems" for Moderate¹³ systems, the Moderate control baseline from NIST SP 800-53 "Recommended Security Controls for Federal Information Systems", and all applicable provisions in MD 12.5 "Automated Information Security Program".

The contractor shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the contractor's computer facility, and the contractor will retain no NRC data within 30 calendar days after contract is completion. Until all data is purged, the contractor shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

All media used by the contractor to store or process NRC information shall be controlled in such a manner as to protect it at the Moderate sensitivity level.

Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 and must be operated in FIPS mode, where validated modules exist. For all FIPS 140-2 cryptographic modules used by the system, 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 contractor shall not publish or disclose in any manner, without the contracting officer's and NRC DDMS Project Officer's written consent, the details of any security controls or countermeasures either designed or developed by the contractor under this contract or otherwise provided by the NRC.

The contractor shall only use government furnished licensed software and in-house developed authorized software (including NRC and contractor developed) on the system and for processing NRC information. Public domain, shareware, or freeware shall not be installed unless authorized by the NRC DDMS Project Officer after he/she has obtained written approval from the NRC Chief Information Security Officer (CISO).

The Contractor shall notify the NRC DDMS Project Officer within 24 hours when it is determined, for any reason, that a Contractor employee no longer requires access to an NRC system.

Two months prior to this contracts ending period of performance, the Contractor shall provide a list of NRC access approved staff that may require continued access to NRC systems either as part of a follow-on contract related to this contract or for other active NRC contracts or task orders. If continued access is required for other active NRC contracts or task orders, the list

¹³ The level of controls needed to meet these requirements is based on the level of information sensitivity as determined by the DDMS Security Categorization Document. The Information Sensitivity level of the DDMS is categorized as moderate.

Digital Data Management System Operations and Maintenance Statement of Work

shall include the name of the NRC Project Officer, NRC Contracting Officer, Contract Number/Task Order, and Contract/Task Order name.

The Contractor shall ensure that the DDMS, and any system that processes NRC information:

- 1) Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to provide,
- 2) Be able to authenticate data that includes information for verifying the claimed identity of individual users (e.g., passwords),
- 3) Protect authentication data so that it cannot be accessed by any unauthorized user,
- 4) Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user,
- 5) Report to appropriate security personnel when attempts are made to guess the authentication data whether inadvertently or deliberately,
- 6) Records the following events:
 - a) Use of identification and authentication mechanisms,
 - b) Introduction of objects into a user's address space (e.g., file open, program initiation),
 - c) Deletion of objects,
 - d) Actions taken by computer operators and system administrators or system security officers,
 - e) Other security relevant events as defined by the CSO,
 - f) Override of security controls,
- 7) Implement auditing, per CSO guidance, for the following:
 - a) All operating systems,
 - b) Application and application servers,
 - c) Web servers,
 - d) Web services,
 - e) Network devices,
 - f) Databases and database servers,
- 8) Has the capability to log, at a minimum, the following events:
 - 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

Digital Data Management System
Operations and Maintenance Statement of Work

v) Output to a printer

8 Meetings and travel

The Contractor and the DDMS Project Management Team shall attend, as required, occasional (approximately two (2) per month) meetings at the NRC's Rockville office or at the Contractor site to discuss maintenance and operational requests, issues, and progress.

9 Period of Performance

The period of performance for this contract shall commence on September 15, 2010 and expire on September 14, 2011 months thereafter. This contract may be extended at the option of the Government for four (4) additional one (1)-year periods.

10 Place of Performance

Efforts under all tasks will be performed at the Contractor site, at the Rockville hearing room, located at:

U.S. Nuclear Regulatory Commission
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

at the Las Vegas NRC Hearing Facility, located at:

Pacific Enterprise Plaza
Building One
3250 Pepper Lane
Las Vegas, NV 89120

or other locations in cities located near nuclear facilities or proposed nuclear facilities throughout the United States or its territories involved in licensing or enforcement activities. See the following NRC Internet web pages for potential locations:

- <http://www.nrc.gov/info-finder/reactor/>
- <http://www.nrc.gov/info-finder/materials/fuel-cycle/>
- <http://www.nrc.gov/info-finder/materials/uranium/>
- <http://www.nrc.gov/waste/ql-waste.html>

11 Contractor Performance Requirements

11.1 Documentation Deliverables

For all written deliverables, models, diagrams, and graphics, the Contractor shall deliver a draft for NRC review and shall deliver further versions until all concerns are addressed to the satisfaction of the NRC DDMS Project Officer via the DDMSwebmaster@nrc.gov e-mail account using the internal NRC e-mail system. All deliverables of this nature shall be delivered to the NRC in electronic form in its native format, such as Microsoft Word, Microsoft Excel, Microsoft Project, etc., as well as in Adobe PDF format.

Digital Data Management System
Operations and Maintenance Statement of Work

11.2 Quality Assurance Surveillance Plan

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

11.2.1 Purpose of the QASP

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

The QASP is intended to accomplish the following:

Define the roles and responsibilities of participating government officials;

Define the types of work to be performed:

1. Describe the evaluation methods that will be employed by the government in assessing the Contractor's performance;
2. Provide copies of the quality assurance monitoring forms that will be used by the government in documenting and evaluating the Contractor's performance; and
3. Describe the process of performance documentation.

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

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

11.2.2 Types of Work Performed

1. Task One – Operations and Maintenance
2. Task Two – IT Related Security Activities
3. Task Three – Hearing/Meeting Support
4. Task Four – Application Enhancements, Development and Test Environment
5. Task Five – Training
6. Optional Tasks

Digital Data Management System Operations and Maintenance Statement of Work

- a. Optional Task 6A - Technology Refresh of Rockville Data Processing Sub-System
- b. Optional Task 6B - Technology Refresh of Las Vegas Data Processing Sub-System
- c. Optional Task 6C - Technology Refresh of Rockville Audio Visual Sub-System
- d. Optional Task 6D - Technology Refresh of Las Vegas Audio Visual Sub-System
- e. Optional Task Seven - Transition Task

11.2.3 Methods of Surveillance

There are several methods of surveillance for the performance requirements outlined in Appendix A that will be utilized. These include:

- Bi-Monthly status reports, user input, project schedule review
- Help desk and webmaster e-mail monitoring
- Inspection of deliverables, verification of schedules, and evidence of communication (i.e. e-mail threads, meeting minutes, etc)
- Inspection of Rational Tools
- NRC DDMS Project Officer review of documentation
- The review of a daily submittal report
- The review of submitted reports
- Training feedback forms and surveys
- User input

11.2.4 Quality Assurance Forms and Report

The Government's Quality Assurance (QA) monitoring, accomplished by the NRC DDMS Project Officer, will be reported using the monitoring form in Appendix B. The form, when completed, will document the NRC DDMS Project Officer's understanding of the Contractor's performance under the contract to ensure that the performance measures are being met. The NRC DDMS Project Officer will retain a copy of all completed QA monitoring forms.

1. The NRC DDMS Project Officer will use the Surveillance Monitoring Form, found in Appendix B, to document and evaluate the Contractor's performance under the contract on a quarterly basis.
2. The NRC DDMS Project Officer will judge each requirement in accordance with the performance standards for each task.
3. The NRC DDMS Project Officer will substantiate all requirements which he/she judges to be indicative of "unacceptable" performance. Performance at the "acceptable" level is expected from the Contractor and need not be substantiated; however, it will be noted on the form.
4. The NRC DDMS Project Officer will forward copies of all completed surveillance monitoring forms to the NRC Contracting Officer and Contractor upon completion of form, quarterly. The Contractor is required to respond in writing to any negative QA monitoring form(s) within five (5) working days after receipt of the form.

Digital Data Management System
Operations and Maintenance Statement of Work

11.2.5 Analysis of Surveillance Results

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

The NRC DDMS Project Officer must coordinate and communicate with the Contractor to resolve issues and concerns of marginal or unacceptable performance. The Contractor shall adjust service accordingly to bring performance up to an acceptable level.

The NRC DDMS Project Officer will notify the Contractor of failure to meet standards through QA monitoring forms.

The NRC Contracting Officer will take action, based on the completed QA monitoring forms in accord with the FAR.

Digital Data Management System
Operations and Maintenance Statement of Work

Appendix A – Performance Requirement

Task One				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Adherence to the NRC PMM.	Follows the NRC's Project Management Methodology and all procedures documented as part of that process.	Documented procedures are followed	Inspection of Rational Tools	Quarterly Incentive Fee of \$2500.00 when the NRC PMM documented procedures are followed
Documentation Updates	Update of DDMS documents based on DDMS configuration management plan, document update schedule (found in the DDMS Table of Documents) and as outline in this SOW.	Documents delivered based on agreed schedule and do not require substantial edits or changes to content.	NRC DDMS Project Officer review of documentation	For each day document updates are delivered late, beyond fourteen (14) days of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Reconciliation of document synchronization between ADAMS and DDMS	Report all discrepancies found during daily data consistency checks	Document synchronization issues are brought to the attention of the NRC DDMS Project Officer by 8:30 am ET as part of the daily submittal report	Review of Daily submittal report	Quarterly Incentive Fee of \$1000.00 when all reports are submitted by 8:30 am ET each day of the quarter.
Verification of nightly Backup and/or resolution of identified issues.	Backups are conducted according to the procedures documented in the DDMS Backup and Recovery Plan	Backup issues are brought to the attention of the Project Office by 8:30 am ET as part of the daily submittal report	Review of Daily submittal report	Quarterly Incentive Fee of \$1000.00 when all reports are submitted by 8:30 am ET each day of the quarter.

Digital Data Management System
Operations and Maintenance Statement of Work

Task One				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/ Disincentive
Ensure site connectivity to include data replication between sites.	DDMS Maintains 99% site connectivity excluding circumstances beyond the Contractors control	Ninety-nine (99) percent site connectivity	Review of Daily submittal report	Quarterly Incentive Fee of \$2500.00 when DDMS maintains 99% site connectivity sites.
Delivery of reports as defined in Section 5.1.7	Delivery of reports as defined in the SOW.	Delivery Schedule set forth in Section 5.1.7 or agreed upon delivery schedule	Review of submitted report	For each day weekly/monthly reports are delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Notification of expiring software or hardware license or maintenance agreements.	Notification of software or hardware license or maintenance agreements that will expire in the following quarter	Notification during the previous quarter.	Review of submitted report	\$1000.00 will be deducted for each software or hardware maintenance or license agreement that is not brought to the attention of the government for renewal the quarter before it expires.

Digital Data Management System
Operations and Maintenance Statement of Work

Task Two				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/Disincentive
Delivery of reports as defined in Section 5.2.4	Delivery of reports as defined in the SOW.	Delivery Schedule set forth in Section 5.2.4 or agreed upon delivery schedule	Review of submitted report	For each day weekly/monthly reports are delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.

Task Three				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/Disincentive
Qualified Personal available to support hearing or meeting.	On site staff can a) operate DDMS sufficiently to support an ASLBP hearing, b) can resolve system issues as they arise as to not disrupt hearing activity, c) can respond to users questions regarding the functional use of DDMS.	Qualified Contractor staff are on site as defined in the SOW	User input	Deduction of \$1000.00 for each event in which the Contractor does not provide adequate staffing

Digital Data Management System
Operations and Maintenance Statement of Work

Task Four				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/Disincentive
Delivery of reports as defined in Section 5.4.4	Delivery of reports as defined in the SOW.	Delivery schedule set forth in Section 5.4.4 or agreed upon delivery schedule	Review of submitted report	For each day weekly/monthly reports are delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Adherence to DDMS Configuration Management procedures	DDMS configuration management procedures are followed as defined in the DDMS Change Control Board Charter and DDMS Configuration Management Plan	Proper procedures followed as defined in the SOW and applicable DDMS documents.	Inspection of deliverables, verification of schedules, and evidence of communication (i.e. e-mail threads, meeting minutes, etc)	For each configuration change made to DDMS not following defined configuration management procedures, \$1000.00 will be deducted from the Contractors invoice.

Digital Data Management System
Operations and Maintenance Statement of Work

Task Five				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/Disincentive
Delivery of reports as defined in Section 5.5.4	Delivery of reports as defined in the SOW.	Delivery schedule set forth in Section 5.5.4 or agreed upon delivery schedule	Review of submitted report	For each day weekly/monthly reports are delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Provide effective training	The Contractor shall provide effective training to the DDMS user community on the functional use of the system.	Ninety (90) percent or better user satisfaction.	Training feedback forms and surveys	Yearly incentive fee of \$2,500.00 for user feedback forms indicating ninety (90) percent or better satisfaction with training provided.
User community trained at appropriate levels to utilize the DDMS	The Contractor shall conduct training for the DDMS user community and provide the sufficient information in a variety of formats which enables the DDMS user community to successfully utilize DDMS during ASLBP proceedings.	Less than five (5) percent user negative feedback.	Help desk and webmaster e-mail monitoring	Yearly incentive fee of \$2,500.00 for less than five (5) percent negative feedback from end users.

Digital Data Management System
Operations and Maintenance Statement of Work

Task Six				
Performance Requirement	Performance Standard	Acceptable Level of Performance	Method of Monitoring	Incentive/Disincentive
Delivery of reports as defined in Section 5.7	Delivery of reports as defined in the SOW.	Delivery schedule set forth in Section 5.7 or agreed upon delivery schedule	Review of submitted report	For each day weekly/monthly reports are delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Delivery of PMM related documentation as defined in Section 5.7	Delivery of PMM related documentation	Delivery schedule set forth in Section 5.7 or agreed upon delivery schedule	Review of submitted documentation	For each day specific documentation is delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Delivery of security related documentation as defined in Section 5.7	Delivery of security related documentation	Delivery schedule set forth in Section 5.7 or agreed upon delivery schedule	Review of submitted documentation	For each day specific documentation is delivered late, beyond one (1) day of the delivery date, \$150 per day will be deducted from the Contractor's invoice.
Technology Refresh Implementation	The implementation of the technology refresh should have a limited impact on the current operational state of the DDMS, meet PMM, CCB, Test and Acceptance, Security Certification and Accreditation and documentation requirements	Schedules as defined in the technology refresh plan are met with less than five (5) percent schedule variance	Bi-Monthly status reports, user input, project schedule review	For each day schedule milestones pass the five (5) percent threshold, \$150.00 per milestone per day will be deducted from the Contractor's invoice.

Appendix B – Surveillance Monitoring Form

Digital Data Management System
Operations and Maintenance Statement of Work

Performance Requirement	Method of Monitoring	Date Review Performed	Compliance	If Unacceptable, State Reason
Task One - Adherence to the NRC PMM.	Inspection of Rational Tools		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task One - Documentation Updates	NRC DDMS Project Officer review of documentation		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task One - Reconciliation of document synchronization between ADAMS and DDMS	Review of Daily submittal report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task One - Verification of nightly Backup and/or resolution of identified issues.	Review of Daily submittal report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task One - Ensure site connectivity to include data replication between sites.	Review of Daily submittal report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task One - Delivery of reports as defined in Section 5.1.7	Review of submitted report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Two - Delivery of reports as defined in Section 5.2.4	Review of submitted report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Three - Qualified Personal available to support hearing or meeting.	User input		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Four - Delivery of reports as defined in Section 5.4.4	Review of submitted report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	

Digital Data Management System
Operations and Maintenance Statement of Work

Performance Requirement	Method of Monitoring	Date Review Performed	Compliance	If Unacceptable, State Reason
Task Four - Adherence to DDMS Configuration Management procedures	Inspection of deliverables, verification of schedules, and evidence of communication (i.e. e-mail threads, meeting minutes, etc)		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Five - Delivery of reports as defined in Section 5.5.4	Review of submitted report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Five - Provide effective training	Training feedback forms and surveys		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Five - User community trained at appropriate levels to utilize the DDMS	Help desk and webmaster e-mail monitoring		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Six - Delivery of reports as defined in Section 5.7	Review of submitted report		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Six - Delivery of PMM documentation as defined in Section 5.7	Review of submitted PMM documentation		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Six - Delivery of security documentation as defined in Section 5.7	Review of submitted security documentation		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	
Task Six - Technology Refresh Implementation	Bi-Monthly status reports, user input, project schedule review		<input type="checkbox"/> Acceptable <input type="checkbox"/> Unacceptable <input type="checkbox"/> Not Applicable	

SYSTEM NAME:

Drug Testing Program Records—NRC.

SYSTEM LOCATION:

Primary system—Division of Facilities and Security, Office of Administration, NRC, Two White Flint North, 11545 Rockville Pike, Rockville, Maryland.

Duplicate system—Duplicate systems exist in part at the NRC Regional office locations listed in Addendum I, Part 2 (for a temporary period of time); and at the current Contractor testing laboratories, collection/evaluation facilities.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Persons including NRC employees, applicants, consultants, licensees, and Contractors.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records contain information regarding the drug testing program; requests for and results of initial, confirmatory and follow-up testing, if appropriate; additional information supplied by NRC employees, employment applicants, consultants, licensees, or Contractors in challenge to positive test results; and written statements or medical evaluations of attending physicians and/or information regarding prescription or nonprescription drugs.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C 7301 (note); 42 U.S.C. 290dd-2; Executive Order 12564; Pub. L. 100-71, Title V Sec. 503; Pub. L. 100-440, Title VI Sec. 628; Executive Order 9397.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to the disclosures permitted under subsection (b) of the Privacy Act, the NRC may disclose information contained in this system of records without the consent of the subject individual if the disclosure is compatible with the purpose for which the record was collected under the following routine uses:

- a. To identify substance abusers within the agency;
- b. To initiate counseling and/or rehabilitation programs;
- c. To take personnel actions;
- d. To take personnel security actions;
- e. For statistical reporting purposes. Statistical reporting will not include personally identifiable information; and
- f. For the routine uses specified in paragraphs number 6 and 7 of the Prefatory Statement of General Routine Uses.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records are maintained on paper and computer media. Specimens are maintained in appropriate environments.

RETRIEVABILITY:

Records are indexed and accessed by name, social security number, testing position number, specimen number, drug testing laboratory accession number, or a combination thereof.

SAFEGUARDS:

Records in use are protected to ensure that access is limited to those persons whose official duties require such access. Unattended records are maintained in NRC-controlled space in locked offices, locked desk drawers, or locked file cabinets. Stand-alone and network processing systems are password protected and removable media is stored in locked offices, locked desk drawers, or locked file cabinets when unattended. Network processing systems have roles and responsibilities protection and system security plans. Records at laboratory, collection, and evaluation facilities are stored with appropriate security measures to control and limit access to those persons whose official duties require such access.

RETENTION AND DISPOSAL:

Records are retained and disposed of in accordance with the National Archives and Records Administration (NARA) approved disposition schedules which can be found in the NRC Comprehensive Records Disposition Schedule, NUREG-0910, NARA's General Records Schedules, as well as in recently approved Requests for Records Disposition Authorities. NRC records disposition schedules are accessible through the NRC's Web site at <http://www.nrc.gov/reading-rm/recordsmgmt/disposition.html>. Records that do not have an approved disposition schedule will be retained until disposition authority is obtained from NARA in accordance with 36 CFR 1220.38(b), Disposition of Records.

SYSTEM MANAGER(S) AND ADDRESS:

Director, Division of Facilities and Security, Office of Administration, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether this system of records contains information about them should write to the Freedom of Information Act and Privacy Act Officer, Office of Information Services, U.S. Nuclear Regulatory Commission, Washington, DC 20555-0001, and comply with the procedures contained in NRC's Privacy Act regulations, 10 CFR part 9.

RECORD ACCESS PROCEDURE:

Same as "Notification procedure."

CONTESTING RECORD PROCEDURE:

Same as "Notification procedure."

RECORD SOURCE CATEGORIES:

NRC employees, employment applicants, consultants, licensees, and Contractors who have been identified for drug testing who have been tested; physicians making statements regarding medical evaluations and/or authorized prescriptions for drugs; NRC Contractors for processing including, but not limited to, specimen collection, laboratories for analysis, and medical evaluations; and NRC staff administering the drug testing program to ensure the achievement of a drug-free workplace.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(5), the Commission has exempted portions of this system of records from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).

**BILLING INSTRUCTIONS FOR
FIXED PRICE 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 the Standard Form 26, Block 25 of the Standard Form 33, or Block 18a. of the Standard Form 1449, whichever is applicable.

**BILLING INSTRUCTIONS FOR
FIXED PRICE CONTRACTS (JUNE 2008)**

Frequency: The contractor shall submit a voucher/invoice only after the NRC's final acceptance of services rendered or products delivered in performance of the contract unless otherwise specified in the contract.

Preparation and Itemization of the Voucher/Invoice: The voucher/invoice shall be prepared in ink or by typewriter (without strike-overs). Corrections or erasures must be initialed. To be considered a proper voucher/invoice, all of the following elements must be included:

1. Contractor's Data Universal Number (DUNS) or DUNS+4 number that identifies the contractor'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 contractor to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.
2. Contract number.
3. Sequential voucher/invoice number.
4. Date of voucher/invoice.
5. 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).
6. A description of articles or services, quantity, unit price, and total amount.
7. For contractor acquired property, list each item with an initial acquisition cost of \$50,000 or more and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.
8. Weight and zone of shipment, if shipped by parcel post.
9. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.
10. Instructions to consignee to notify the Contracting Officer of receipt of shipment.
11. For Indefinite Delivery contracts or contracts under which progress payments are authorized, the final voucher/invoice shall be marked "FINAL VOUCHER" OR "FINAL INVOICE."

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

Supersession: These instructions supersede any previous billing instructions.

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

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.

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.

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

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.

3. Definitions

- a. Non-capitalized Equipment, Materials, and Supplies. These are equipment other than that described in

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

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
Direct Costs:		
(1) Direct Labor	\$ _____	\$ _____
		-
(2) Travel	\$ _____	\$ _____
		-
(3) Materials	\$ _____	\$ _____
		-
(4) Equipment	\$ _____	\$ _____
		-
(5) Materials Handling Fee	\$ _____	\$ _____
		-
(6) Consultants	\$ _____	\$ _____
		-
(7) Subcontracts	\$ _____	\$ _____
		-
Total Direct Costs:	\$ _____	\$ _____
		-

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

CONTRACT SECURITY AND/OR CLASSIFICATION REQUIREMENTS

COMPLETE CLASSIFIED ITEMS BY SEPARATE CORRESPONDENCE

1. CONTRACTOR NAME AND ADDRESS

TBD

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

TBD

B. PROJECTED START DATE

09/15/2010

C. PROJECTED COMPLETION DATE

09/14/2010

2. TYPE OF SUBMISSION



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

NRC-D2-21-10-496

DATE

09/14/2010

4. PROJECT TITLE AND OTHER IDENTIFYING INFORMATION

Enterprise Digital Data Management System Operations and Maintenance

5. PERFORMANCE WILL REQUIRE

A. ACCESS TO CLASSIFIED MATTER OR CLASSIFIED INFORMATION

YES (If "YES," answer 1-7 below)

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



NO

C. UNESCORTED ACCESS IS REQUIRED TO NUCLEAR POWER PLANTS.

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

D. ACCESS IS REQUIRED TO UNCLASSIFIED SAFEGUARDS INFORMATION.

H. WILL OPERATE HAZARDOUS EQUIPMENT AT NRC FACILITIES.

E. ACCESS IS REQUIRED TO SENSITIVE IT SYSTEMS AND DATA.

I. REQUIRED TO CARRY FIREARMS.

F. UNESCORTED ACCESS TO NRC HEADQUARTERS BUILDING.

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 <p style="text-align: center;">Andrew Welkie DDMS Project Manager</p>	SIGNATURE 	DATE <p style="text-align: center;">02/16/2010</p>
---	---	--

7. CLASSIFICATION GUIDANCE

NATURE OF CLASSIFIED GUIDANCE IDENTIFICATION OF CLASSIFICATION GUIDES

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

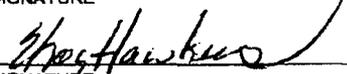
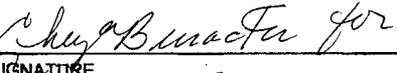
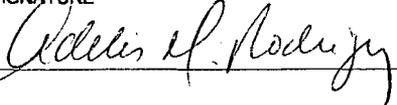
AUTHORIZED CLASSIFIER (Name and Title)
 DIVISION OF FACILITIES AND SECURITY

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

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

10. APPROVALS

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

NAME (Print or type)	SIGNATURE	DATE
A. DIRECTOR, OFFICE OR DIVISION E. Roy Hawkens	SIGNATURE 	DATE 18 FEB 10
B. DIRECTOR, DIVISION OF FACILITIES AND SECURITY Robert B. Webber	SIGNATURE 	DATE 4/12/10
C. DIRECTOR, DIVISION OF CONTRACTS AND PROPERTY MANAGEMENT (Not applicable to DOE agreements) Phyllis A. Bower	SIGNATURE 	DATE 4/12/10

REMARKS