B.1 PERFORMANCE WORK SCHEDULE

PERFORMANCE WORK STATEMENT (PWS)
NRC META SYSTEM HELP DESK

I. BACKGROUND

The Nuclear Regulatory Commission (NRC) has initiated a project to develop the means, through process change and technology improvement, to receive and manage complex, electronic document submittals in anticipation of major license applications such as new nuclear power plants and license renewals for existing nuclear power plants. During the course of performing activities to prepare for and support these major licensing programs, the NRC has identified a collection of business processes and information technology/information management components known as the NRC Meta System. The NRC Meta System will receive, process, and distribute documents submitted by nuclear power plant licensees and the Department of Energy (DOE). The following NRC business processes and information environment components comprise the NRC Meta System:

- Receive License Application information
- Process License Application Information
- Manage the Docket
- Perform Technical Analysis
- Manage the Adjudicatory Hearings
- Manage the Libraries (NRC information collections)
- Electronic Information Exchange (EIE)
- NRC Local Area Network(LAN)/Wide Area Network(WAN/Internet
- NRC Email
- Agency-wide Document Access and Management System (ADAMS)
  - ADAMS Main Library
  - Web-based Search for ADAMS Main Library
- Electronic Hearing Docket (EHD)
  - Web-based Search for EHD (EIP)
- Publicly Available Records System (PARS)
  - Citrix Based Interface
  - Public Interface Portal (PIP)

While individual components of the NRC Meta System have implemented end-user support, an Information Management gap identifies the need to implement end-user support from the NRC Meta System perspective by establishing a NRC Meta System Help Desk. To that end, a call center must be established that supports the following activities:

a. Responding to requests for assistance – The primary role of the NRC Meta System Help Desk is to provide a principal point of contact for NRC staff, the parties and participants in licensing activities, and the general public. Contact methods must include toll-free telephone service and response to email inquiries. For the purposes of this document, "calls" are synonymous with "requests for assistance" whether the "calls" are received via the telephone or via email.

- Receive calls for assistance

- Record problem information
- Resolve the problem
- Document call resolution
- Solicit and evaluate customer feedback
- Identify recurring problems
- Monitor system operability from an end-user perspective

b. Escalation of unresolved requests for assistance to NRC Tier 2 support entities through the development of an escalation process and method. The NRC Tier 2 support entities include the NRC Contracting Officer Representative and the Business Analyst contractor. The process for escalation shall be a detailed email to the COR stating the issue and assistance required, then a telephone call if no email response is received within an hour of the initial email. This activity shall also include a customer call back for all escalated calls to ensure the customer knows the issue has been escalated.

c. Nature of expected requests for assistance - The following is a brief description of calls, either by telephone or email, that the Contractor may reasonably expect to receive:

- Calls for assistance on information search and retrieval from NRC document collections - PARS, EHD/EIP, ADAMS/SIP
- Calls for assistance based on customer questions about published support documentation such as software installation instructions, user guides, FAQs
- Calls for assistance with EIE, EHD, including administrative issues
- Calls for assistance associated with ADAMS, NRC Email, NRC Network, the Internet, NRC workstations
- Calls for assistance associated with the NRC electronic submittal guidance "**Guidance for Electronic Submissions to the NRC**", including assistance in conversion of NRC adjudicatory documents to acceptable formats such as Adobe® Portable Document Format (PDF)
- Calls from the NRC Document Processing Center (DPC) to ask for assistance with the customer to resolve rejected electronic document submittals. This interaction would include advice to customers whose documents are rejected by the DPC of the NRC settings for PDF documents and communicate to the customer the basis for document rejection.

II. PERFORMANCE-BASED SCOPE OF WORK

The Contractor shall operate the NRC Meta System and the NRC licensing activities, as described in Section I of this Performance Work Statement (PWS). The Contractor shall plan, design, implement, operate, and manage the contact center and associated services to meet the needs of the Government.

III. SPECIFIC TASKS

Through the NRC Meta System Help Desk task, the Contractor shall:

a. Provide interested citizens and the parties and participants to the NRC licensing activities with responses to their inquiries.
b. Note operational data about technical, functional, or business process areas of the supported systems that could benefit from improvement in status reports. Operational data may include, but not limited to, system slowness, system errors, or customer feedback on workflows.
c. Provide a call center solution to meet the requirements identified in this PWS.

IV. DELIVERABLES AND DELIVERY DATES

Hours of Operation (Responding to Telephone and Email Inquiries)

The hours of operation for requests for assistance from the NRC Meta System Help Desk are identified in Table 1 below according to program phases. The Contractor may perform work that does not require real-time response during non-business hours (e.g., responding to email inquiries, transcribing voice mail messages), provided that such arrangement does not adversely affect performance objectives and the Government's ability to communicate its needs with the Contractor. The Contractor may be required to provide expanded telephone and email coverage to include the periods indicated in Table 1 below.

Table 1 – NRC Meta System Help Desk Hours of Operation (Telephone and Email Inquiries)		
Program Phase	Weekday Coverage (Eastern Time)	
	Day Coverage	Night Coverage
Daily Support	9:00 am to 7:00 pm	As Needed 7:00 pm* to 12:00 am
The Principal Period of service is Monday through Friday from 9 a.m. until 7 p.m. (EST). This will be billed as CLIN 1. The Non-Principal Period of service is on an as needed basis as requested in writing by the COR. The contractor will be given at a minimum of five business days written notice from the COR when night coverage will be needed for a particular day. The total number of nights needed is estimated at five total nights (7:00 pm – 12:00 am) per task order year.		

Management Plans

The Contractor shall provide the following management plans in accordance with the schedule set forth in Section 2.0 of this PWS and additional documents will be identified as a result of these plans. The contents of the documents shall conform to the descriptions of the documents as described in this section. The Contractor shall review all documents on a continual basis throughout the life of the task order in order to maintain their accuracy and appropriateness to the current operating environment. Subsequent to their initial acceptance by the COR, any changes to these plans shall require COR review and COR written approval prior to their implementation. The documents to be provided by the Contractor include:

a. Customer Satisfaction Plan
b. Disaster Recovery/Contingency Plan
c. Knowledge\Case Management Plan
d. Operations Management Plan
e. Performance/Service Level Management Plan
f. Phase-In Plan
g. Program Management Plan
h. Project Plan
i. Quality Assurance/Quality Improvement Program Plan
j. Test and Acceptance Plan

Management Plan Descriptions

Customer Satisfaction Plan - identifies plans and procedures to survey customers to determine the degree of customer satisfaction on the services rendered. The plan shall include details on the processes and methodologies that the offeror will use to identify problems and implement corrective actions.

Disaster Recovery/Contingency Plan – identifies every risk as well as the steps necessary to prevent it from happening in the first place. The plan shall include an alternate set of steps to minimize the impact should prevention fail. The plan must define backup and restoration processes and the precise steps to take to recover as quickly as possible, including recovery procedures for physical facility, voice, data, and desktop systems and

applications, communications networks, electrical service, customer access points, partners and procedures and staff. The Plan shall define the roles and responsibilities of contractor personnel during contingent and disaster events, including plans for training the personnel to prepare them to respond to such events. The plan shall include implementation procedures to test and execute the plan on a regular basis to ensure preparedness for such events. The plan shall be developed in accordance with applicable agency IT Security Policy and NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems.

Knowledge/Case Management Plan - identifies methodologies, processes and procedures for effective knowledge management, including those required for developing, operating, and maintaining the required knowledge and case management databases to support the contact center operations. Where appropriate, the plan shall include methodologies and procedures for effective management of distributed knowledge databases and sharing of knowledge/case management data with other government and/or contractor systems. The Knowledge/Case Management Plan shall include a configuration management plan, address system configuration documentation, and provide a change management plan that follows NRC change control policies, procedures, and describes the role of the Information System Security Officer (ISSO).

Operations Management Plan – identifies plans and procedures for managing staff, facilities, equipment and processes effectively; includes procedures that the Contractor shall follow in the event of a service outage, an unexpected surge in call volume, a Federal Government closure or other emergency affecting the area in which the contact centers is located.

Performance Management Plan – identifies plans and procedures to measure any customer service performance standards deemed appropriate.

Phase-In Plan – identifies plans and approaches for implementing the proposed solution, including required tasks, schedule and milestones, and deliverables. The plan shall include methodologies and procedures for minimizing disruption of service to current customers.

Program Management Plan – identifies and defines the Contractor's organization, roles and responsibilities, and lines of authority, management procedures/policies/plans, plans and programs for managing team partners and subcontractors, escalation procedures for problem/dispute resolution, and reporting requirements for the tasks and services to be performed under this task order.

Project Plan – provides a comprehensive plan for implementing the task order, which addresses all strategies, objectives, required actions, roles and responsibilities and target dates for implementation of tasks. The Project Plan identifies critical paths and task dependencies and includes a Decommissioning Plan for information resources produced during execution of the task order.

Quality Assurance/Quality Improvement Program Plan – identifies plans, methodologies, and procedures for maintaining effective quality assurance and service improvement programs, including monitoring and assessing performance and service activities to ensure quality services are provided to customers. Included in the program shall be a Quality Improvement Plan to identify and document performance assessment and improvement opportunities and procedures for implementing the service improvements. The Plan shall address all areas, including, staffing, training, operations, contract deliverables, performance management, process engineering, service delivery, service improvements, and customer satisfaction.

Service Level Management Plan – identifies processes and methodologies for effective service level management, including workload forecasting, IS scheduling, service recovery (from system failures, disasters, etc.), problem identification and resolution, problem notification, and contingency planning and escalation.

Test and Acceptance Plan – identifies plans and procedures that the contractor shall use to ensure that the full range of services to be provided are successfully tested prior to actual implementation. The Contractor shall provide documentation of the tests performed and the test results.

Management Reports

The Contractor shall generate and provide status and issues reports that meet the requirements detailed below. The COR intends to request and receive only those reports that provide insight to the Contractor's level of performance in meeting contractual requirements and satisfying customer needs. The COR may also request the Contractor to provide management and operational reports on an ad hoc basis for purposes of gaining insight to specific program and customer service needs. Specific report formats, content, frequency, and delivery methods of all reports shall be coordinated with, and approved by the COR. The Contractor shall provide management reports via a secure website for remote access and download via the Internet by the COR, and when requested, in hard copy and/or electronic format.

Such reports are not considered and counted as ad hoc reports as described in this section. Reports shall be provided on a weekly basis to the COR with daily and monthly summaries, as applicable for the reported activities. Daily reports, when requested, are due the following business day. Weekly reports are due within two (2) business days after the conclusion of each week. Monthly reports are due within five (5) business days after the conclusion of each month. The COR may provide these reports to other individuals.

The Contractor shall provide task order status and contact center performance including, but not limited to:

Task Order Status Reports must include, at a minimum:

- List of Work Performed during the reporting period
- List of Activities anticipated for the next reporting period
- Call/Inquiry/E-mail Activities
- Service Levels/Quality
- Inquiry/Request Types and Trends
- Exceptions
- Notification of Service Outages
- Management Reporting
- Problems/Issues and Trends
- Notification of Changes
- Performance Assessment Reports

Ad Hoc Reports

Throughout the base period and for each of the option periods, the COR may request up to twelve (12) reports on an ad hoc basis, and in cases of non-performance, more detailed and frequent reports, at no additional cost to the government.

Business Documents

The Contractor shall obtain and provide all permits, contracts, copyrights, licenses, etc. necessary for the performance of the requirements of this task order and shall provide copies of such information to the COR upon request.

Other Deliverables

The Contractor shall provide the following deliverables in accordance with the schedule set forth in Table 3 below. The content of these plans shall conform to the descriptions contained in this PWS and additional deliverable schedules will be identified as a result of these plans. The deliverables shall be provided in

Microsoft Word, Microsoft PowerPoint, Excel, or Microsoft Project format, as appropriate, and in hard copy. The Contractor shall review all plans on a continual basis throughout the life of the task order in order to maintain their accuracy and appropriateness to the current operating environment. Subsequent to their initial acceptance by the COR, any changes to these plans shall require COR review and approval prior to their implementation.

All documents and reports delivered under this task order shall be provided in the specified format. Deliverables under this task order will be reviewed by the COR for completeness and accuracy. The COR will accept or reject the deliverables in writing within 10 working days from date of receipt.

V. PERIOD OF PERFORMANCE

The period of performance of this contract is (1) one Base Year plus six (6) one (1) year options to extend the term of the task order. The term of this contract may be extended at the option of the Government for an additional 6 years pursuant to clause 52.217-9.

Base Period – December 1, 2012 to November 30, 2013
Option Year 1 – December 1, 2013 to November 30, 2014
Option Year 2 – December 1, 2014 to November 30, 2015
Option Year 3 – December 1, 2015 to November 30, 2016
Option Year 4 – December 1, 2016 to November 30, 2017
Option Year 5 – December 1, 2017 to November 30, 2018
Option Year 6 – December 1, 2018 to November 30, 2019

VI. PLACE OF PERFORMANCE

The Government will provide the facilities at NRC Headquarters required to support the requirements identified within this PWS.

VII. PERFORMANCE STANDARDS

This section outlines the primary and secondary performance indicator metrics for the NRC Meta System Help Desk task. The Contractor shall perform all task requirements in such a way that they meet or exceed the performance levels and sample calculations specified in Table 2 below for each of the supported services.

Table 2 – Performance Requirements Summary

Performance Indicator	Sample Calculation *(Actual calculations to be determined during Contract negotiations)*	Expected Target Performance*	Frequency of Measure/ Reporting	Incentive or disincentive
a. Response Time				
1. Service Level (Telephone Inquiries)	(Calls answered within 20 seconds + Calls abandoned within 20 seconds)/(Total calls answered + Total calls abandoned)	80% within 20 seconds	Daily/ Monthly	Decrease in monthly payment for labor equal to the percentage of missed performance target
2. Email Response Time Part A	(Emails responded to and/or closed within 1 or 2 business days)/Total emails received)	90% within 1 business days	Daily/ Monthly	5% Reduction of amount payable for monthly invoice

Table 2 – Performance Requirements Summary				
Performance Indicator	Sample Calculation *(Actual calculations to be determined during Contract negotiations)*	Expected Target Performance*	Frequency of Measure/ Reporting	Incentive or disincentive
3. Email Response Time Part B	(Emails responded to and/or closed within 1 or 2 business days)/Total emails received)	100% within 2 business days	Daily/ Monthly	10% Reduction of amount payable for monthly invoice
b. Quality Assurance				
1. Deliverables	Deliverables reviewed and accepted by the Government without substantive corrective action.	100%	Per Deliverable Schedule	Contractor performs corrective actions for deliverables
c. Customer Satisfaction				
1. Customer Survey - Email	(Number of inquirers responded favorably to survey / Total number of inquirers solicited)	90% or better	Monthly / Quarterly	Decrease in monthly payment of 1% of monthly charges for each 10% below target – applied as a discount during the subsequent quarter
2. Service Availability	(Total time service is not available during that month (in minutes)) / (Total time in the month)	99.9%	Daily/ Monthly	Decrease in monthly payment for the entire (cumulative number of minutes or hours) that service is not available during the month

VIII. GOVERNMENT- FURNISHED PROPERTY, DATA AND/OR INFORMATION

The Government will furnish pertinent information to the Contractor for use in the performance of the NRC Meta System Help Desk task. Examples of information available include the following:

a. Initial content for knowledge database (current FAQs)
b. Business rules, response formats, guidelines, and preformatted responses
c. Examples of email responses
d. Escalation procedures and guidelines
e. Contact listing for NRC Tier 2 support entities
f. NRC IT systems security policy and guidelines
g. Reference materials
h. Office supplies

For any materials to be distributed to the inquiring public, the Contractor shall submit written re-supply requests to the COR ensure continuous availability.

The Contractor shall provide and maintain technology infrastructures that it provides NRC to support the requirements identified in this PWS. This includes inquiry processing technology and services, email routing and management system, FAQ updates, knowledge management system, contact management system, work force management system, service monitoring and quality control systems, training equipment, voice mail and electronic mail systems, and power supplies. Call processing and Email routing and management systems shall incorporate automated capabilities to perform periodic checks on the systems to verify operational status of the contractor systems, or agency and other contractor systems, or both, and alert contractor's system

maintenance personnel and/or the Government if there is a failure. The Contractor shall keep all system documentation up to date.

a. Information Systems Security

The Contractor shall be accountable commensurate with the risks inherent with the information sensitivity under the latest National Institute of Standards and Technologies (NIST) Federal Information Processing (FIPS) Standards and Special Publications (SP) 800 Series guidance.

The Contractor shall ensure that its data communications are secured to (encryption, authentication, data integrity checking, key exchange, and data compression) commensurate with the risks inherent with the information sensitivity.

All system modifications must comply with NRC security policies and procedures for a high sensitivity system, as well as federal laws, guidance, and standards to ensure FISMA compliance and NRC's MD 12.5 "NRC Automated Information Security Program."

The contractor shall ensure that its personnel, in performance of the contract, receive IT security training in their role (e.g. system administrators must received training in the IT security of the operating system being used).

The contractor shall not publish or disclose in any manner, without the contracting officer's written consent, the details of any protections either designed or developed by the contractor under this task order or otherwise provided by the government.

The contractor agrees to abide by NRC regulations for handling sensitive unclassified information governed by the NRC's Sensitive Unclassified Non-Safeguards Information program (SUNSI) and NRC's MD 12.5, "NRC Automated Information Security Program."

The contractor shall only use NRC-provided e-mail accounts to send and receive information considered to be personally identifiable information (PII) or shall use other NRC approved encrypted means (e.g., secure ZIP, encrypted e-mails).

Separation of duties for the systems must be enforced by the system through assigned access authorizations.

The information system shall provide only essential capabilities and specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

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

The contractor shall only use licensed software and in-house developed authorized code (including government and contractor developed) on the on the system and for processing government information. Public domain, shareware, or freeware shall only be installed after prior written approval is obtained from the COR. The contractor shall provide proof of licensing upon request of the Contracting Officer, or the COR,
All development and testing of the systems shall be performed on a network separate and isolated from the NRC operational network that is protected at the high sensitivity level.

All system computers must be properly configured and hardened (up to date with all anti-virus software and Microsoft security patches) to NRC standards, and comply with all NRC security policies.

User accounts that have system-level or administrative privileges must have a unique password from all other accounts held by that user, and general user tasks must be performed from a general user account, not from the administrative account.

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

All sensitive data being transmitted over a network by the system shall use FIPS 140-2 validated encryption. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

All media produced must include appropriate markings to indicate the sensitivity of the information contained on the media and the media must be controlled according that that sensitivity.

The Contractor shall meet the Continuous Monitoring requirements identified in NIST Special Publication 800-37.

b. NRC META SYSTEM HELP DESK Knowledge Database

The NRC Meta System Help Desk core mission is to support parties and participants to the NRC licensing activities and minimize delays to the hearing process. In order to perform this function, the contractor is required to establish and maintain a knowledge database to support the services described in this PWS, including a library of "preformatted responses" used to respond to requests for assistance. The Contractor shall also maintain a library of "previous good answers" that the NRC Meta System Help Desk personnel can access and use to respond to similar requests. The Contractor shall continuously monitor the inquiry trends and make additions, deletions, or modifications to the library of preformatted responses and "previous good answers" to enhance the response process. To the maximum extent possible, the Contractor shall ensure that the knowledge management system leverages the use of the same information across all supported services. The Contractor is responsible for validating the accuracy of the knowledge database and updating the information on an ongoing basis to ensure that the information in the knowledge database remains current.

c. Contact Management System Design

The Contractor shall provide and maintain an inquiry tracking system to track all relevant inquiry activities to support the services described in this PWS. At a minimum, the Contractor shall track the information identified below. The Contractor shall work with the COR to identify the appropriate information to track for the NRC Meta System Help Desk task to meet NRC objectives. The calls must be identified as pertinent to the anticipated Yucca Mountain Project (YMP) licensing activities or general licensing activities.

1) Inquirer's name
2) Inquirer's mailing address
3) Inquirer's telephone number
4) Inquirer's Zip Code
5) Inquirer's fax number
6) Inquirer's email address
7) Type of inquiry (e.g. phone, email)
8) Inquiry tracking number
9) Date inquiry received
10) Time inquiry received
11) Date/Time inquiry forwarded to a Tier 2 support entity
12) Delivery status of inquiry forwarded to a Tier 2 support entity
13) Date inquiry responses processed by the Contractor
14) Time inquiry responses processed by the Contractor
15) Delivery status of inquiry responses processed by the Contractor
16) Date(s) inquiry cleared (closed out) by Contractor
17) Time(s) inquiry cleared (closed out) by Contractor
18) Subject of inquiry (entered by IS or customer or both)

19) Subject of inquiry (selected by IS or customer)
20) Nature/subject of inquiry
21) Information embedded in mail messages generated via a web email form
22) Action(s) taken by Contractor
23) Nature of response action needed
24) Name(s) of a Tier 2 support entity inquiry is forwarded to
25) Issue Resolution Description

The system shall be capable of accepting outside input in order to update certain fields (such as the "Date email cleared by the Contractor" field). The Contractor shall enter "N/A" into any field without data (e.g., "Date closed by Contractor" when the response is processed by the Contractor itself). Data input to these fields may be done manually or by batch files.

The system shall be expandable to add additional fields and/or entries as required by the COR.

d. Access to Knowledge Management and Contact Management Systems

For quality audit and program management purposes, the Contractor shall provide access to its task order management systems to the COR.

B.2 PRICE/COST SCHEDULE

Item No.	Description	Qty	Unit	Unit Price	Amount
0001	Base Period: Services required by the Performance Work Statement	12	MO	$	$
1001	Option Period 1: Services required by the Performance Work Statement	12	MO	$	$
2001	Option Period 2: Services required by the Performance Work Statement	12	MO	$	$
3001	Option Period 3: Services required by the Performance Work Statement	12	MO	$	$
4001	Option Period 4: Services required by the Performance Work Statement	12	MO	$	$
5001	Option Period 5: Services required by the Performance Work Statement	12	MO	$	$
6001	Option Period 6: Services required by the Performance Work Statement	12	MO	$	$

B.3 DELIVERABLE SCHEDULE

Table 3	
Deliverable	**Due Date* / Update Frequency****
a. Customer Satisfaction Plan *	30 days / Annual
b. Disaster Recovery/Contingency Plan	30 days / Annual
c. Knowledge/Case Management Plan *	75 days / Annual
d. Operations Management Plan	15 days before operational transition / Annual
e. Performance/Service Level Management Plan *	30 days / Annual
f. Phase-In Plan	20 days before operational transition / As needed
g. Program Management Plan *	30 days / Annual
h. Project Plan *	10 days / As needed
i. Quality Assurance/Quality Improvement Program Plan *	75 days / Annual
j. Security Plan	10 days after Certification and Accreditation Plan / Quarterly
k. Test and Acceptance Plan	15 days after design review / Annual
l. Various Status, Operational and Management Reports ***	Daily/Weekly/Monthly
* Due Date is calendar days after the issuance of the task order	
** Plans must be updated more frequently if there have been fundamental changes since the last update (e.g., a new	

Table 3	
Deliverable	**Due Date* / Update Frequency****
site location, new software, a change in key personnel) *** All status, operational and management reports provided by the contractor are described in this SOW and shall not contain any restrictive markings prohibiting the Government from releasing the information in whole or in part.	

SECTION C - CONTRACT CLAUSES

C.1 ELECTRONIC PAYMENT (AUG 2011)

The Debt Collection Improvement Act of 1996 requires that all payments except IRS tax refunds be made by Electronic Funds Transfer. Payment shall be made in accordance with FAR 52.232-33, entitled "Payment by Electronic Funds- Central Contractor Registration".

To receive payment, the contractor shall prepare invoices in accordance with NRC's Billing Instructions. Claims shall be submitted on the payee's letterhead, 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." The preferred method of submitting invoices is electronically to the Department of the Interior at NRCPayments_NBCDenver@nbc.gov. If the contractor submits a hard copy of the 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

C.2 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (AUG 2011)

The contractor must identify all individuals selected to work under this contract. The NRC Contracting Officer's Representative (COR) shall make the final determination of the level, if any, of IT access approval required for all individuals working under this contract/order using the following guidance. The Government shall have full and complete control and discretion over granting, denying, withholding, or terminating IT access approvals for contractor personnel performing work under this contract/order.

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

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) 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 (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) 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 employee verify the pre-screening record or review, sign

and date it. The contractor shall supply two (2) copies of the signed contractor's pre-screening record or review to the NRC Contracting Officer's Representative (COR), who will then provide them to the NRC Office of Administration, Division of Facilities and Security, Personnel Security Branch with the employee's completed IT access application package.

The contractor shall further ensure that its personnel complete all IT access approval security applications required by this clause within fourteen (14) calendar days of notification by the NRC Contracting Officer's Representative (COR) of initiation of the application process. Timely receipt of properly completed records of the pre-screening record and IT access approval applications (submitted for candidates that have a reasonable probability of obtaining the level of security assurance necessary for access to NRC's IT systems/data) is a requirement of this contract/order. Failure of the contractor to comply with this requirement may be a basis to terminate the contract/order for cause, 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.

SECURITY REQUIREMENTS FOR IT LEVEL I

Performance under this contract/order will involve contractor personnel 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.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary IT access may be approved by DFS/PSB based on a favorable review or adjudication of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably review or adjudication of a completed background investigation. 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/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor shall assign another contractor employee to perform the necessary work under this contract/ order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the contract/order. When an individual receives final IT access approval from DFS/PSB, the individual will be subject to a reinvestigation every ten (10) years thereafter (assuming continuous performance under contract/order at NRC) or more frequently in the event of noncontinuous performance under contract/order at NRC.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to the NRC PO who will then provide them to DFS/PSB for review and adjudication, prior to the individual being authorized to perform work under this contract/order requiring access to sensitive information technology systems or data. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than seven (7) years residency in the U.S. will not be approved for IT Level I access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor individual may be denied access to NRC facilities and sensitive information technology systems or data until a final determination is made by DFS/PSB and thereafter communicated to the contractor by the NRC Contracting Officer's Representative (COR) regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level I contractors shall be subject to the attached NRC Form 187 and SF-86 which furnishes the basis for providing security requirements to contractors that 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/order 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.

Contractor personnel shall not have access to sensitive information technology systems or data until they are approved by DFS/PSB and they have been so informed in writing by the NRC Contracting Officer's Representative (COR). Temporary access may be approved by DFS/PSB based on a favorable review of their security forms and checks. Final IT access may be approved by DFS/PSB based on a favorably adjudication. However, temporary access authorization approval will be revoked and the contractor 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/order requiring IT access without the approval of DFS/PSB, as communicated in writing to the contractor by the NRC Contracting Officer's Representative (COR). Where temporary access authorization has been revoked or denied by DFS/PSB, the contractor is responsible for assigning another contractor employee to perform the necessary work under this contract/order without delay to the contract/order performance schedule, or without adverse impact to any other terms or conditions of the contract/order. When a contractor employee receives final IT access approval from DFS/PSB, the individual will be subject to a review or reinvestigation every ten (10) years (assuming continuous performance under contract/order at NRC) or more frequently in the event of noncontinuous performance under contract/order at NRC.

The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, through the NRC Contracting Officer's Representative (COR) to DFS/PSB for review and adjudication, prior to the contractor employee being authorized to perform work under this contract/order. Non-U.S. citizens must provide official documentation to the DFS/PSB, as proof of their legal residency. This documentation can be a Permanent Resident Card, Temporary Work Visa, Employment Authorization Card, or other official documentation issued by the U.S. Citizenship and Immigration Services. Any applicant with less than seven (7) years residency in the U.S. will not be approved for IT Level II access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB. The contractor shall ensure that all forms are accurate, complete, and legible. Based on DFS/ PSB review of the contractor employee's security forms and/or the receipt of adverse information by NRC, the contractor employee may be denied access to NRC facilities, sensitive information technology systems or data until a final determination is made by DFS/PSB regarding the contractor person's eligibility.

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187, SF-86, and contractor's record of the pre-screening which furnishes the basis for providing security requirements to contractors that 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 NRC Contracting Officer's Representative (COR) by telephone so that the access review may be promptly discontinued. The

notification shall contain the full name of the contractor employee and the date of the request. Telephone notifications must be promptly confirmed by the contractor in writing to the NRC Contracting Officer's Representative (COR), who will forward the confirmation to DFS/PSB. Additionally, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) in writing, who will in turn notify DFS/PSB, when a contractor employee no longer requires access to NRC sensitive automated information technology systems or data, including the voluntary or involuntary separation of employment of a contractor employee who has been approved for or is being processed for IT access.

The contractor shall flow the requirements of this clause down into all subcontracts and agreements with consultants for work that requires them to access NRC IT resources.

C.3 INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS - GENERAL (JULY 2011)

INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS - GENERAL

Basic Contract IT Security Requirements

For unclassified information used for the effort, the contractor shall provide an information security categorization document indicating the sensitivity of the information processed as part of this contract if the information security categorization was not provided in the statement of work. The determination shall be made using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 and must be approved by CSO. The NRC contracting officer and Contracting Officer's Representative (COR) shall be notified immediately before the contractor begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the NRC contracting officer and Contracting Officer's Representative (COR) shall be notified before the contractor begins to process information at a more restrictive classification level.

All work under this contract shall comply with the latest version of policy, procedures and standards. Individual task orders will reference latest versions of standards or exceptions as necessary. These policy, procedures and standards include: NRC Management Directive (MD) volume 12 Security, Computer Security Office policies, procedures and standards, 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. This information is available at the following links:

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

NRC Policy and Procedures For Handling, Marking and Protecting Sensitive Unclassified Non-Safeguards Information (SUNSI): http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf

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

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

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

The Contractor shall ensure compliance with the latest version of NIST guidance and FIPS standards available at contract issuance and continued compliance with the latest versions within one year of the release date.

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 CSO.

All Contractor employees must sign the NRC Agency-Wide Rules of Behavior for Authorized Computer Use prior to being granted access to NRC computing resources.

The Contractor shall adhere to following NRC policies:

1. Management Directive 12.5, Automated Information Security Program
2. NRC Sensitive Unclassified Non-Safeguards Information (SUNSI)
3. Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
4. Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
5. Computer Security Information Protection Policy
6. Remote Access Policy
7. Use of Commercial Wireless Devices, Services and Technologies Policy
8. Laptop Security Policy
9. Computer Security Incident Response Policy

Contractor will adhere to NRC's prohibition of use of personal devices to process and store NRC sensitive information.

All electronic process of NRC sensitive information, including system development and operations and maintenance performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the highest sensitivity of the information that is processed or will ultimately be processed.

Contract Performance And Closeout

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. Tools used to perform data purging shall be approved by the CISO. The contractor shall provide written certification to the NRC contracting officer that the contractor does not retain any NRC data within 30 calendar days after contract 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.

When contractor employees no longer require access to an NRC system, the contractor shall notify the Contracting Officer's Representative (COR) within 24 hours.

Upon contract completion, the contractor shall provide a status list of all contractor employees who were users of NRC systems and shall note if any users still require access to the system to perform work if a follow-on contract or task order has been issued by NRC.

Control Of Information And Data

The contractor shall not publish or disclose in any manner, without the contracting 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.

Any IT system used to process NRC sensitive information shall:

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.

Access Controls

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

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

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

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

2. SGI Information - All SGI being transmitted over a network shall adhere to guidance in MD 12.7 NRC Safeguards Information Security Program and MD 12.5 NRC Automated Information Security Program. SGI processing shall be only within facilities, computers, and spaces that have been specifically approved for SGI processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

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

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

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

Configuration Standards

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

Media Handling

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

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

Vulnerability Management

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

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

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

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

C.4 INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS - GENERAL EXCEPTIONS (JULY 2011)

INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS - GENERAL EXCEPTIONS

All purchases shall comply with the latest version of policy, procedures and standards. Individual task orders will reference latest versions of policy, procedures, standards or exceptions as necessary. These policy, procedures and standards include: NRC Management Directive (MD) volume 12 Security, Computer Security Office policies, procedures and standards, 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. This information is available at the following links:

All procurements must be certified and accredited prior to being placed into an operational state.

All electronic processing of NRC sensitive information, including all system development and operations and maintenance activities performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the highest sensitivity of the information that is processed or will ultimately be processed.

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

C.5 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS (AUG 2011)

Annual and final evaluations of contractor performance under this contract will be prepared in accordance with FAR Subpart 42.15, "Contractor Performance Information," normally at or near 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 Contracting Officer's Representative's (COR) 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 and submit comments, rebutting statements, or additional information.

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 "Source Selection Information", 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 and 42.1503. 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.

C.7 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS (AUG 2011)

NRC contractors are responsible to ensure that their alien personnel are not in violation of United States immigration 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 Permanent Resident Form I-551 (Green Card), or must present other evidence from the U.S. Department of Homeland Security/U.S. Citizenship and Immigration Services that employment will not affect his/her immigration status. The U.S. Citizenship and Immigration Services provides information to contractors to help them understand the employment eligibility verification process for non-US citizens. This information can be found on their website, http://www.uscis.gov/ portal/site/uscis.

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.

C.8 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS (AUG 2011)

Review and Approval of Reports

(a) Reporting Requirements. The contractor/grantee shall comply with the terms and conditions of the contract/grant regarding the contents of the draft and final report, summaries, data, and related documents, to include correcting, deleting, editing, revising, modifying, formatting, and supplementing any of the information contained therein, at no additional cost to the NRC. Performance under the contract/grant will not be deemed accepted or completed until it complies with the NRC's directions. The reports, summaries, data, and related documents will be considered draft until approved by the NRC. The contractor/ grantee agrees that the direction, determinations, and decisions on approval or disapproval of reports, summaries, data, and related documents created under this contract/grant remain solely within the discretion of the NRC.

(b) Publication of Results. Prior to any dissemination, display, publication, or release of articles, reports, summaries, data, or related documents developed under the contract/grant, the contractor/grantee shall submit them to the NRC for review and approval. The contractor/ grantee shall not release, disseminate, display or publish articles, reports, summaries, data, and related documents, or the contents therein, that have not been reviewed and approved by the NRC for release, display, dissemination or publication. The contractor/grantee agrees to conspicuously place any disclaimers, markings or notices, directed by the NRC, on any articles, reports, summaries, data, and related documents that the contractor/grantee intends to release, display, disseminate or publish to other persons, the public, or any other entities. The contractor/grantee agrees, and grants, a royalty-free, nonexclusive, irrevocable worldwide license to the government, to use, reproduce, modify, distribute, prepare derivative works, release, display or disclose the articles, reports, summaries, data, and related documents developed under the contract/grant, for any governmental purpose and to have or authorize others to do so.

(c) Identification/Marking of Sensitive Unclassified Non-Safeguards Information (SUNSI) and Safeguards Information (SGI). The decision, determination, or direction by the NRC that information possessed, formulated or produced by the contractor/grantee constitutes SUNSI or SGI is solely within the authority and discretion of the NRC. In performing the contract/grant, the contractor/grantee shall clearly mark SUNSI and SGI, to include for example, OUO-Allegation Information or OUO-Security Related Information on any reports, documents, designs, data, materials, and written information, as directed by the NRC. In addition to marking the information as directed by the NRC, the contractor shall use the applicable NRC cover sheet (e.g., NRC Form 461 Safeguards Information) in maintaining these records and documents. The contractor/grantee shall ensure that SUNSI and SGI is handled, maintained and protected from unauthorized disclosure, consistent with NRC policies and directions. The contractor/grantee shall comply with the requirements to mark, maintain, and protect all information, including documents, summaries, reports, data, designs, and materials in accordance with the provisions of Section 147 of the Atomic Energy Act of 1954 as amended, its implementing regulations (10 CFR 73.21), Sensitive Unclassified Non-Safeguards and Safeguards Information policies, and NRC Management Directives and Handbooks 12.5, 12.6 and 12.7.

(d) Remedies. In addition to any civil, criminal, and contractual remedies available under the applicable laws and regulations, failure to comply with the above provisions, and/or NRC directions, may result in suspension, withholding, or offsetting of any payments invoiced or claimed by the contractor/grantee.

(e) Flowdown. If the contractor/grantee intends to enter into any subcontracts or other agreements to perform this contract/grant, the contractor/grantee shall include all of the above provisions in any subcontracts or agreements.

C.9 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (AUG 2011)

(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 entitled: "Your Rights Under the Energy Reorganization Act".

(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.

C.10 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (AUG 2011)

Prior to occupying any government provided space at NRC HQs in Rockville Maryland, the Contractor shall obtain written authorization to occupy specifically designated government space, via the NRC Contracting Officer's Representative (COR), from the Chief, Space Design Branch, ADSPC. Failure to obtain this prior authorization can result in one, or a combination, of the following remedies as deemed appropriate by the Contracting Officer.

(1) Rental charge for the space occupied will be deducted from the invoice amount due the Contractor

(2) Removal from the space occupied

(3) Contract Termination

C.11 GREEN PURCHASING (JUN 2011)

(a) In furtherance of the sustainable acquisition goals of Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance" products and services provided under this contract/order shall be energy- efficient (Energy Star or Federal Energy Management Program (FEMP) designated), water-efficient, biobased, environmentally preferable (e.g., Electronic Product Environmental Assessment Tool (EPEAT) certified), non-ozone depleting, contain recycled content, or are non-toxic or less toxic alternatives, where such products and services meet agency performance requirements. http://www.fedcenter.gov/programs/eo13514/

(b) The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order.

C.12 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS (AUG 2011)

The Debt Collection Improvement Act of 1996 requires that all Federal payments except IRS tax refunds be made by Electronic Funds Transfer. It is the policy of the Nuclear Regulatory Commission to pay government vendors by the Automated Clearing House (ACH) electronic funds transfer payment system. Item 15C of the Standard Form 33 may be disregarded.

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

NONE PROVIDED

SECTION E - SOLICITATION PROVISIONS

E.1 GREEN PURCHASING (JUN 2011)

COST PROPOSAL-COVER PAGE

The offeror's cost proposal shall include the following information to identify the major category that best represents the environmental products and services included in the proposal, as applicable.

In the offeror's cost proposal cover page, select the most prominent green category from the list provided below and provide a corresponding total dollar amount for the category.

"The preponderance of green purchasing included in this proposal includes:

Category:_____ (Select the most prominent green category, only)

Dollar Amount: $_____." (Offerors may include $0 for IDIQs, Requirements contracts and other contract vehicles where the actual work will be implemented through the award of task or delivery orders.)

Select Only One of the Following Categories:

A. Recycled Content Products

B. Energy-Efficient Products: Energy Star, FEMP-Designated, and Low Standby Power Devices

C. Biobased Products

D. Environmentally Preferable Products and Services (excluding EPEAT)

E. Electronic Product Environmental Assessment Tool (EPEAT) Products

F. Water-Efficient Products

G. SNAP/Non-Ozone Depleting Substances

H. Alternative Fuel Vehicles and Alternative Fuels

I. Not Applicable

A listing of designated EPA products can be found at: http://www.epa.gov/epawaste/conserve/tools/cpg/index.htm