

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>		BPA NO.	1. CONTRACT ID CODE	PAGE 1 OF 19
2. AMENDMENT/MODIFICATION NO. M001	3. EFFECTIVE DATE See Block 16c	4. REQUISITION/PURCHASE REQ. NO. NRC-HQ-12-C-38-0079-M001		5. PROJECT NO. (if applicable)
6. ISSUED BY U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Rob Robinson, 301-492-3693 Mail Stop: TWB-01-B10M Washington, DC 20555	CODE 3100	7. ADMINISTERED BY (if other than item 6) U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555		CODE 3100
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)  BATTLE RESOURCE MANAGEMENT, INC. BRMI  5525 ADAMS RIDGE RD CLARKSVILLE MD 210291171		(X)	9A. AMENDMENT OF SOLICITATION NO.	
			9B. DATED (SEE ITEM 11)	
			10A. MODIFICATION OF CONTRACT/ORDER NO. NRC-HQ-12-C-38-0079	
		X	10B. DATED (SEE ITEM 13) 07-03-2012	
CODE	FACILITY CODE			

### 11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

- ☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.
- Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:
- (a) By completing Items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (if required) B&R#: 2012-84-51-H-192; Job Code: T8491; BOC 251A  
Appro.#: 31X0200; NAICS Code: 541990; DUNS#: 15-128-8037

### 13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(X)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(p).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

**E. IMPORTANT:** Contractor ☐ is not, ☒ is required to sign this document and return \_\_\_\_\_ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

The purpose of this modification is to add security related contract clauses to the base contract.

Total Estimated Cost: \$950,000.00 (unchanged)  
Total Obligated Amount: \$25,000.00 (unchanged)  
Period of Performance: July 3, 2012 - September 30, 2012 (unchanged)

Please see attached pages for specific contract changes and added clauses.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print) KAREN FONES, Director Financial Ops	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Erika Eam Contracting Officer
15B. CONTRACTOR/OFFEROR K. Fones	15C. DATE SIGNED 7/25/12
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	16B. UNITED STATES OF AMERICA BY Erika Eam (Signature of Contracting Officer)
	16C. DATE SIGNED 7/25/2012

NSN 7540-01-152-8070  
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)  
Prescribed by GSA - FAR (48 CFR) 53.243

**SUNSI REVIEW COMPLETE**

JUL 30 2012

TEMPLATE - ADM001

ADM002

***The following clauses are hereby incorporated in their entirety to SECTION C – CONTRACT CLAUSES of the Base Contract, NRC-HQ-12-C-38-0079:***

**“C.30 SECURITY REQUIREMENTS FOR BUILDING ACCESS APPROVAL (AUG 2011)**

The Contractor shall ensure that all its employees, subcontractor employees or consultants who are assigned to perform the work herein for contract performance for periods of more than 30 calendar days at NRC facilities, are approved by the NRC for unescorted NRC building access.

The Contractor shall conduct a preliminary federal facilities security screening interview or review for each of its employees, subcontractor employees, and consultants and submit to the NRC only the names of candidates for contract performance that have a reasonable probability of obtaining approval necessary for access to NRC's federal facilities. 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 applicant verify the pre-screening record or review, sign and date it. Two (2) copies of the pre-screening signed record or review shall be supplied to the Division of Facilities and Security, Personnel Security Branch (DFS/PSB) 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 building access security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed records of the Contractor's signed pre-screening record or review and building access security applications (submitted for candidates that have a reasonable probability of obtaining the level of access authorization 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.

A Contractor, subcontractor employee or consultant shall not have access to NRC facilities until he/she is approved by DFS/PSB. Temporary access may be approved based on a favorable NRC review and discretionary determination of their building access security forms. Final building access will be approved based on favorably adjudicated checks by the Government. However, temporary access approval will be revoked and the Contractor's employee may subsequently be denied access in the event the employee's investigation cannot be favorably determined by the NRC. Such employee will not be authorized to work under any NRC contract requiring building access without the approval of DFS/PSB. When an individual receives final access, the individual will be subject to a review or reinvestigation every five (5) or ten (10) years, depending on their job responsibilities at the NRC.

The Government shall have and exercise full and complete control and discretion over granting, denying, withholding, or terminating building access approvals for individuals performing work under this contract. Individuals performing work under this contract at NRC facilities for a period of more than 30 calendar days shall be required to complete and submit to the Contractor representative an acceptable OPM Standard Form 85 (Questionnaire for Non-Sensitive Positions), and two (2) FD 258 (Fingerprint Charts). 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 five (5) years residency in the U.S. will not be approved for building access. The Contractor shall submit the documents to the NRC Contracting Officer's Representative (COR) who will give them to DFS/PSB.

DFS/PSB may, among other things, grant or deny temporary unescorted building access approval to an individual based upon its review of the information contained in the OPM Standard Form 85 and the Contractor's pre-screening record. Also, in the exercise of its authority, the Government may, among other things, grant or deny permanent building access approval based on the results of its review or investigation. This submittal requirement also applies to the officers of the firm who, for any reason, may visit the NRC work sites for an extended period of time during the term of the contract. In the event that DFS/PSB are unable to grant a temporary or permanent building access approval, to any individual performing work under this contract, the Contractor is responsible for assigning another individual to perform the necessary function without any delay in the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The Contractor is responsible for informing those affected by this procedure of the required building access approval process (i.e., temporary and permanent determinations), and the possibility that individuals may be required to wait until permanent building access approvals are granted before beginning work in NRC's buildings.

#### **CANCELLATION OR TERMINATION OF BUILDING ACCESS/ REQUEST**

The Contractor shall immediately notify the PO when a Contractor or subcontractor employee or consultant's need for NRC building access approval is withdrawn or the need by the Contractor employee's for building access terminates. The PO will immediately notify DFS/PSB (via e-mail) when a Contractor employee no longer requires building access. The Contractor shall be required to return any NRC issued badges to the Contracting Officer's Representative (COR) for return to DFS/PSB (Facilities Security Branch) within three (3) days after their termination.

### **C.31 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 favorable 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.

**NRC-HQ-12-C-38-0079**  
**M001**

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 favorable 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.32 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/>

**NRC-HQ-12-C-38-0079**  
**M001**

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 be 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.33 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.34 IT SECURITY REQUIREMENTS - DEVELOPMENT AND OPERATIONS AND MAINTENANCE REQUIREMENTS (JULY 2011)**

#### **IT SECURITY REQUIREMENTS - DEVELOPMENT AND OPERATIONS AND MAINTENANCE REQUIREMENTS**

##### **O&M Security Requirements**

All system modifications to classified systems must comply with NRC security policies and procedures for classified systems, as well as federal laws, guidance, and standards to ensure Federal Information Security Management Act (FISMA) compliance.

The Contractor shall correct errors that are discovered by the NRC or the contractor in contractor developed software and applicable documentation that are not commercial off-the-shelf which are discovered by the NRC or the contractor. Inability of the parties to determine the cause of software errors shall be resolved in accordance with the Disputes clause, FAR 52.233-1, Incorporated by reference in the contract.

The Contractor shall adhere to the guidance outlined in NIST, SP 800-53, FIPS 200 and NRC guidance for the identification and documentation of minimum security controls.

The contractor shall provide the system requirements traceability matrix at the end of the initiation phase, development/acquisition phase, implementation/ assessment phase, operation & maintenance phase and disposal phase that provides the security requirements in a separate section so that they can be traced through the development life cycle. The contractor shall also provide the software and hardware designs and test plan documentation, and source code upon request to the NRC for review.

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

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

All contractor provided deliverables identified in the project plan will be subject to the review and approval of NRC Management. The PM will establish review time based on the complexity of the system and incorporate into the project schedule. The contractor will make the necessary modifications to project deliverables to resolve any identified issues. Project deliverables include but are not limited to: requirements, architectures, design documents, test plans, and test reports.

System development schedules shall include computer security office go/no-go decision points, including but not limited to the following system milestones:

1. Requirements review
2. Architecture review
3. Detailed design review
4. Code review
5. System test
6. System readiness review

### Access Controls

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

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

### Cryptography

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. 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.

### Configuration Management And Control

The contractor must ensure that the system will be divided into configuration items (CIs). CIs are parts of a system that can be individually managed and versioned. The system shall be managed at the CI level.

The contractor must have a configuration management plan that includes all hardware and software that is part of the system and contains at minimum the following sections:

1. Introduction
  - a. Purpose & Scope
  - b. Definitions
  - c. References
2. Configuration Management
  - a. Organization
  - b. Responsibilities
  - c. Tools and Infrastructure
3. Configuration Management Activities
  - a. Specification Identification
  - b. Change control form identification
  - c. Project baselines
4. Configuration and Change Control
  - a. Change Request Processing and Approval
  - b. Change Control Board
5. Milestones
  - a. Define baselines, reviews, audits
  - b. Training and Resources

The Information System Security Officer's (ISSO's) role in the change management process must be described. The ISSO is responsible for the security posture of the system. Any changes to the system security posture must be approved by the ISSO. The contractor should not have the ability to make changes to the system's security posture without the appropriate involvement and approval of the ISSO.

**NRC-HQ-12-C-38-0079**  
**M001**

The contractor shall track and record information specific to proposed and approved changes that minimally include:

1. Identified configuration change
2. Testing of the configuration change
3. Scheduled implementation the configuration change
4. Track system impact of the configuration change
5. Track the implementation of the configuration change
6. Recording & reporting of configuration change to the appropriate party
7. Back out/Fall back plan
8. Weekly Change Reports and meeting minutes
9. Emergency change procedures
10. List of team members from key functional areas

The contractor shall provide a list of software and hardware changes in advance of placing them into operation within the following timeframes:

- 30 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 10 calendar days for a low sensitivity system

The contractor must maintain all system documentation that is current to within:

- 10 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

Modified code, tests performed and test results, issue resolution documentation, and updated system documentation shall be deliverables on the contract.

Any proposed changes to the system must have written approval from the NRC Contracting Officer's Representative (COR).

The contractor shall maintain a list of hardware, firmware and software changes that is current to within:

- 15 calendar days for a classified, SGI or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

The contractor shall analyze proposed hardware and software configurations and modification as well as addressed security vulnerabilities in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

**NRC-HQ-12-C-38-0079**  
**M001**

The contractor shall provide the above analysis with the proposed hardware and software for NRC testing in advance of NRC accepted operational deployment dates within:

- 15 calendar days for a classified, SGI, or high sensitivity system
- 20 calendar days for a moderate sensitivity system
- 30 calendar days for a low sensitivity system

**Control Of Hardware And Software**

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

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

**Auditing**

The system shall be able to create, maintain and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected so that read access to it is limited to those who are authorized.

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

The Contractor shall ensure auditing is implemented on the following:

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

The contractor shall perform audit log reviews daily using automated analysis tools. In addition, the contractor must log at least the following events on systems that process NRC information:

- Audit all failures
- Successful logon attempt
- Failure of logon attempt
- Permission Changes
- Unsuccessful File Access
- Creating users & objects
- Deletion & modification of system files
- Registry Key/Kernel changes
- Startup & shutdown
- Authentication
- Authorization/permission granting
- Actions by trusted users

- Process invocation
- Controlled access to data by individually authenticated user
- Unsuccessful data access attempt
- Data deletion
- Data transfer
- Application configuration change
- Application of confidentiality or integrity labels to data
- Override or modification of data labels or markings
- Output to removable media
- Output to a printer

## **C.35 IT SECURITY REQUIREMENTS - CERTIFICATION AND ACCREDITATION (MAR 2011)**

### **IT SECURITY REQUIREMENTS - CERTIFICATION AND ACCREDITATION**

#### **SECURITY RISK ASSESSMENT**

The contractor shall work with the NRC Contracting Officer's Representative (COR) 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, 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 develop the system security plan (SSP) according to NRC policy, standards, and guidance to define the implementation of IT security controls necessary to meet both the functional assurance and security requirements. The contractor will ensure that all controls required to be implemented are documented in the SSP.

#### **ASSESSMENT PROCEDURES - SECURITY TEST & EVALUATION**

The contractor shall follow NRC policy, standards, and guidance for execution of the test procedures. These procedures shall be supplemented and augmented by tailored test procedures based on the control objective as it applies to NRC. The contractor shall include verification and validation to ensure that appropriate corrective action was taken on identified security weaknesses.

The contractor shall perform ST&E activities, including but not limited to, coordinating the ST&E and developing the ST&E Plan, execution ST&E test cases and documentation of test results. The contractor shall prepare the Plan of Action and Milestones (POA&M) based on the ST&E results.

#### **PLAN OF ACTION AND MILESTONES (POA&M) MAINTENANCE & REPORTING**

The contractor shall provide a determination, in a written form agreed to by the NRC Contracting Officer's Representative (COR) and Computer Security Office, on whether the implemented corrective action was adequate to resolve the identified information security weaknesses and provide the reasons for any exceptions or risk-based decisions. The contractor shall document any vulnerabilities indicating which portions of the security control have not been implemented or applied.

The contractor shall develop and implement solutions that provide a means of planning and monitoring corrective actions; define roles and responsibilities for risk mitigation; assist in identifying security funding requirements; track and prioritize resources; and inform decision-makers of progress of open POA&M items.

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

#### **CERTIFICATION & ACCREDITATION DOCUMENTATION**

The contractor shall create, update maintain all Certification and Accreditation (C&A) documentation in accordance with the following NRC Certification and Accreditation procedures and guidance:

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

The Contractor must develop contingency plan and ensure annual contingency testing is completed within one year of previous test and provide an updated security plan and test report according to NRC's policy and procedure.

The Contractor must conduct annual security control testing according to NRC's policy and procedure and update POA&M, SSP, etc. to reflect any findings or changes to management, operational and technical controls.

### **C.36 IT SECURITY REQUIREMENTS - NRC AND CONTRACTOR (NON-NRC) FACILITIES (MAR 2011)**

#### **IT SECURITY REQUIREMENTS - NRC AND CONTRACTOR (NON-NRC) FACILITIES**

##### **BACKUPS**

The contractor shall ensure that backup media is created, encrypted (in accordance with information sensitivity) and verified to ensure that data can be retrieved and is restorable to NRC systems based on information sensitivity levels. Backups shall be executed to create readable media that allows successful file/data restoration at the following frequencies:

- At least every 1 calendar day for a high sensitivity system
- At least every 1 calendar day for a moderate sensitivity system
- At least every 7 calendar days for a low sensitivity system

##### **PERIMETER PROTECTION**

The Contractor must employ perimeter protection mechanisms, such as firewalls and routers, to deny all communications unless explicitly allowed by exception.

The contractor must deploy and monitor intrusion detection capability and have an always deployed and actively engaged security monitoring capability in place for systems placed in operation for the NRC. Intrusion detection and monitoring reports will be 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

#### **CONTRACTOR FACILITY REVIEW AND APPROVAL PROCESS**

The contractor shall complete a security survey of the proposed facility in accordance with MD 12.1 in order for NRC to determine the adequacy and effectiveness of the administration of the security program and the protection afforded NRC information, employees, and assets before the facility is used for any NRC effort that includes IT.

Upon facility approval per MD 12.1, the contractor shall perform a full certification and obtain accreditation of the facility and computing systems that will be used by the contractor as part of the NRC effort that includes IT prior to commencing the effort. The certification shall be performed at the level of the highest sensitivity of the data that is used at the facility or will ultimately be used by the product of the effort.

#### **C.37 SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION (AUG 2011)**

Performance under this contract will require access to classified matter or information (National Security Information or Restricted Data) in accordance with the attached NRC Form 187 (See List of Attachments). Prime Contractor personnel, subcontractors or others performing work under this contract shall require a "Q" security clearance (allows access to Top Secret, Secret, and Confidential National Security Information and Restricted Data) or an "L" security clearance (allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data).

The Contractor must identify all individuals to work under this contract. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

The Contractor shall conduct a preliminary security interview or review for each of its employees, subcontractor employees and consultants, and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed. The Contractor will pre-screen applicants for the following:

(a) pending criminal charges or proceedings; (b) felony arrest records including alcohol related arrest within the last seven (7) years; (c) record of any military courts-martial charges and proceedings in the last seven (7) years and courts-martial convictions in the last ten (10) years; (d) any involvement in hate crimes; (e) involvement in any group or organization that espouses extra-legal violence as a legitimate means to an end; (f) dual or multiple citizenship including the issuance of a foreign passport in the last seven (7) years; (g) illegal use possession, or distribution of narcotics or other controlled substances within the last seven (7) years; (h) financial issues regarding delinquent debts, liens, garnishments, bankruptcy and civil court actions in the last seven (7) years.

The Contractor will make a written record of their pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (h)), and have the candidate verify the record, sign and date it. Two (2) copies of the signed interview record or review will be supplied to DFS/PSB with the applicant's completed security application package.

The Contractor will further ensure that all Contractor employees, subcontractor employees and consultants for classified information access approval complete all security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed security applications (submitted for candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed) is a contract requirement. Failure of the Contractor to comply



with this condition 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 termination or cancellation, the Government may select another firm for contract award.

Such Contractor personnel shall be subject to the NRC Contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation (SSBI) for "Q" clearances or a favorably adjudicated Access National Agency Check and Inquiries (ANACI), or higher level investigation depending on the position the individual will occupy, for "L" clearances.

A Contractor employee shall not have access to classified information until he/she is granted a security clearance by DFS/PSB, based on a favorably adjudicated investigation. In the event the Contractor employee's investigation cannot be favorably adjudicated, any interim access approval could possibly be revoked and the individual could be subsequently removed from performing under the contract. If interim approval access is 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. The individual will be subject to a reinvestigation every five (5) years for "Q" clearances and every ten (10) years for "L" clearances.

The Contractor shall submit a completed security forms packet, including the SF-86, "Questionnaire for National Security Positions," and fingerprint charts, through the PO to DFS/PSB for review and submission to the Office of Personnel Management for investigation. The individual may start working under this contract before a final clearance is granted if a temporary access determination can be made by DFS/PSB after the review of the security package. If the individual is granted a temporary access authorization, the individual may not have access to classified information under this contract until DFS/PSB has granted them the appropriate security clearance, and the Contractor has read, understood, and signed the SF 312, "Classified Information Nondisclosure Agreement." The Contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the Contractor in a sealed envelope), as set forth in NRC MD 12.3. Based on DFS/PSB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3, E.O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204-70 cleared Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments), MD 12.3, SF- 86 and Contractor's signed record or review of the pre-screening which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others who have or may have an NRC contractual relationship which requires access to classified information.

#### **CANCELLATION OR TERMINATION OF SECURITY CLEARANCE ACCESS/REQUEST**

When a request for clearance investigation is to be withdrawn or canceled, the Contractor shall immediately notify the PO by telephone so that the investigation may be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing by the Contractor to the PO who will forward the confirmation via email to DFS/PSB. Additionally, DFS/PSB must be immediately notified in writing when an individual no longer requires access to Government classified information, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC "Personnel Security Program."

### **C.38 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.39 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (AUG 2011)**

All contractor employees, subcontractor employees, and consultants proposed for performance or performing under this contract shall be subject to pre- assignment, random, reasonable suspicion, and post-accident drug testing applicable to: (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 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. 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>."

***All Other Terms and Conditions Remain Unchanged.***