ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 36 PAGES

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

1. DATE OF ORDER	2. CONTRACT NO. (If any)
02/27/2014	GS35F0229K

3. ORDER NO.	4. REQUISITION/REFERENCE NO
NRC-HQ-7S-14-T-0001	See Schedule

5. ISSUING OFFICE (Address correspondence to)
US NRC - HQ
DIVISION OF CONTRACTS
MAIL STOP 3WFN-05-C64MP
WASHINGTON DC 20555-0001

6. SHIP TO:

a. NAME OF CONSIGNEE
US NUCLEAR REGULATORY COMMISSION-

b. STREET ADDRESS
MAIL PROCESSING CENTER
4930 BOILING BROOK PARKWAY

c. CITY	d. STATE	e. ZIP CODE
ROCKVILLE	MD	20852

7 TO. DANIEL HACKENBERG

f SHIP VIA

a. NAME OF CONTRACTOR
MAR INCORPORATED

b. COMPANY NAME

c. STREET ADDRESS
1803 RESEARCH BOULEVARD
SUITE 204

d. CITY	e. STATE	f. ZIP CODE
ROCKVILLE	MD	208506106

8. TYPE OF ORDER

☐ a. PURCHASE
REFERENCE YOUR:

Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

☒ b. DELIVERY

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

9. ACCOUNTING AND APPROPRIATION DATA
See Schedule

10 REQUISITIONING OFFICE
COMPUTER SECURITY OFFICE

11. BUSINESS CLASSIFICATION (Check appropriate box(es))
☒ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date)	16. DISCOUNT TERMS
a. INSPECTION	b. ACCEPTANCE			
Destination	Destination		03/07/2014	

17. SCHEDULE (See reverse for Rejections)

ITEM NO (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Accounting Info: 2014-X0200-FEEBASED-7S-7SD001-51-J-145-N7343-252A Period of Performance: 03/07/2014 to 03/06/2015 Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages)

21. MAIL INVOICE TO

SEE BILLING INSTRUCTIONS ON REVERSE

a. NAME: US NUCLEAR REGULATORY COMMISSION

b. STREET ADDRESS (or P.O. Box): ONE WHITE FLINT NORTH
11555 ROCKVILLE PIKE
MAILSTOP O3-E17A

c. CITY	d. STATE	e. ZIP CODE
ROCKVILLE	MD	20852-2738

$1,940,795.80

17(h) TOTAL (Cont. pages)

17(i) GRAND TOTAL

$1,940,795.80

22. UNITED STATES OF AMERICA BY (Signature)
02/27/2014

23. NAME (Typed)
HERIBERTO COLON
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

AUG 15 2014 ADM002

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
02/27/2014	GS35F0229K	NRC-HQ-7S-14-T-0001

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
00001	Incremental Funding for the CISSS Contract (DR-33-06-317 TO71) $31K for CSO/CSA APT $50K for CSO/CSA IR Award Type: Labor-hour Line Item Ceiling$1,940,795.80 Incrementally Funded Amount: $291,000.00 Requisition No: CSO-14-0007, CSO-14-0014 The obligated amount of award: $291,000.00. The total for this award is shown in box 17(i).				1,940,795.80	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $1,940,795.80

Contents

SECTION B - SUPPLIES OR SERVICES/PRICES

B.1 CONSIDERATION AND OBLIGATION -TASK ORDERS

(a) The ceiling of this order for the services is **$1,940,795.80.**

(b) This order is subject to the minimum and maximum ordering requirements set forth in the contract GS35F0229K.

(c) The amount presently obligated with respect to this order is **$291,000.00**. The obligated amount shall, at no time, exceed the order ceiling as specified in paragraph (a) above. When and if the amount(s) paid and payable to the Contractor hereunder shall equal the obligated amount, the Contractor shall not be obligated to continue performance of the work unless and until the Contracting Officer shall increase the amount obligated with respect to this order, in accordance with FAR Part 43 - Contract Modifications. Any work undertaken by the Contractor in excess of the obligated amount specified above is done so at the Contractor's sole risk and may not be reimbursed by the Government.

(d) The Contractor shall comply with the provisions of FAR 52.232-22 - Limitation of Funds, for incrementally-funded delivery orders or task orders.

SECTION D - PACKAGING AND MARKING

D.1 BRANDING

The Contractor is required to use the statement below in any publications, presentations, articles, products, or materials funded under this contract/order, to the extent practical, in order to provide NRC with recognition for its involvement in and contribution to the project. If the work performed is funded entirely with NRC funds, then the contractor must acknowledge that information in its documentation/presentation.

Work Supported by the U.S. Nuclear Regulatory Commission (NRC), Office of Computer Security, under Contract/order number (see page 1 of this order).

SECTION E - INSPECTION AND ACCEPTANCE

E.1 INSPECTION AND ACCEPTANCE BY THE NRC (SEP 2013)

Inspection and acceptance of the deliverable items to be furnished hereunder shall be made by the NRC Contracting Officer's Representative (COR) at the destination, accordance with FAR 52.247-34 - F.o.b. Destination.

Contract Deliverables:

1. See Attachment 1 – Statement of Work

SECTION F - DELIVERIES OR PERFORMANCE

F.1 TASK/DELIVERY ORDER PERIOD OF PERFORMANCE (SEP 2013)

This order shall commence on March 7, 2014 and will expire on March 6, 2015.

F.2 PLACE OF DELIVERY-REPORTS

The items to be furnished hereunder shall be delivered, with all charges paid by the Contractor, to:

a. Primary and Alternate Contracting Officer's Representatives (COR) (hardcopy or email as directed)

See names and addresses in Section H.3

b. Contracting Officer (CO) (1 copy – via email)

Joseph L. Widdup

Email to: Joseph. Widdup@nrc.gov

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 ELECTRONIC PAYMENT (SEP 2013)

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 Transfer-System Award Management".

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: OCFO ObligationsResource@nrc.gov.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 2052.204-70 SECURITY (OCT 1999)

(a) Security/Classification Requirements Form. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified information or matter, access on a continuing basis (in excess of 90 or more days) to NRC Headquarters controlled buildings, or otherwise requires NRC photo identification or card-key badges.

(b) It is the contractor's duty to safeguard National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for safeguarding National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract upon completion or termination of this contract.

(1) The contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained if the retention is:

(i) Required after the completion or termination of the contract; and

(ii) Approved by the contracting officer.

(2) The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

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

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security and the Contracting Officer. These changes will be

under the authority of the FAR Changes clause referenced in Section I of this document.

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

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

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

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

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

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

(k) In performing contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued under the contract that involves originating or generating classified documents, material, and equipment must provide that the subcontractor or supplier assign the proper classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

H.2 2052.204-71 SITE ACCESS BADGE REQUIREMENTS (JAN 1993)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available as required. In this regard, all contractor personnel whose duties under this contract require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the Government. The COR shall assist the contractor in obtaining the badges for contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has proper identification at all times. All prescribed identification must be immediately delivered to the Security Office for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel shall have this identification in their possession during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

H.3 2052.215-71 CONTRACTING OFFICER'S REPRESENTATIVE AUTHORITY (OCT 1999)

(a) The contracting officer's authorized representatives hereinafter referred to as the Contracting Officer's Representatives (COR) for this contract are:

Primary Contracting Officer's Representative:

Name:	William Dabbs
Address:	Two White Flint North, Mail Stop: TWFN/ 2 D9 11545 Rockville Pike Rockville, MD 20852-2738
Telephone Number:	301-415-0524
Email:	william.dabbs@nrc.gov

Alternate Contracting Officer's Representatives:

Name:	Kathy Lyons-Burke
Address:	Two White Flint North, Mail Stop: TWFN/ 2 D13 11545 Rockville Pike Rockville, MD 20852-2738
Telephone Number:	301-415-6595
Email:	kathy.lyons-burke@nrc.gov

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

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

(2) Provide advice and guidance to the contractor in the preparation of drawings, specifications, or technical portions of the work description.

(3) Review and, where required by the contract, approve technical reports, drawings, specifications, and technical information to be delivered by the contractor to the Government under the contract.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

H.4 2052.222-70 NONDISCRIMINATION BECAUSE OF AGE (JAN 1993)

It is the policy of the Executive Branch of the Government that:

(a) Contractors and subcontractors engaged in the performance of Federal contracts may not, in connection with the employment, advancement, or discharge of employees or in connection with the terms, conditions, or privileges of their employment, discriminate against persons because of their age except upon the basis of a bona fide occupational qualification, retirement plan, or statutory requirement; and

(b) That contractors and subcontractors, or persons acting on their behalf, may not specify, in solicitations or advertisements for employees to work on Government contracts, a maximum age limit for employment unless the specified maximum age limit is based upon a bona fide occupational qualification, retirement plan, or statutory requirement.

H.5 AWARD NOTIFICATION AND COMMITMENT OF PUBLIC FUNDS

(a) All offerors will receive preaward and postaward notices in accordance with FAR 15.503.

(b) It is also brought to your attention that the contracting officer is the only individual who can legally obligate funds or commit the NRC to the expenditure of public funds in connection with this procurement. This means that unless provided in a contract document or specifically authorized by the contracting officer, NRC technical personnel may not issue contract modifications, give formal contractual commitments, or otherwise bind, commit, or obligate the NRC contractually. Informal unauthorized commitments, which do not obligate the NRC and do not entitle the contractor to payment, may include:

(1) Encouraging a potential contractor to incur costs prior to receiving a contract;

(2) Requesting or requiring a contractor to make changes under a contract without formal contract modifications;

(3) Encouraging a contractor to incur costs under a cost-reimbursable contract in excess of those costs contractually allowable; and

(4) Committing the Government to a course of action with regard to a potential contract,

(2) Use, Ownership, and Nondisclosure. A contractor may use NRC owned or controlled PII solely for purposes of this contract, and may not collect or use such PII for any purpose outside the contract without the prior written approval of the NRC Contracting Officer. The contractor must restrict access to such information to only those contractor employees who need the information to perform work under this contract, and must ensure that each such contractor employee (including subcontractors' employees) signs a nondisclosure agreement, in a form suitable to the NRC Contracting Officer, prior to being granted access to the information. The NRC retains sole ownership and rights to its PII. Unless the contract states otherwise, upon completion of the contract, the contractor must turn over all PII in its possession to the NRC, and must certify in writing that it has not retained any NRC owned or controlled PII except as otherwise authorized in writing by the NRC Contracting Officer.

(3) Security Plan. When applicable, and unless waived in writing by the NRC Contracting Officer, the contractor must work with the NRC to develop and implement a security plan setting forth adequate procedures for the protection of NRC owned or controlled PII as well as the procedures which the contractor must follow for notifying the NRC in the event of any security breach. The plan will be incorporated into the contract and must be implemented and followed by the contractor once it has been approved by the NRC Contracting Officer. If the contract does not include a security plan at the time of contract award, a plan must be submitted for the approval of the NRC Contracting Officer within 30 days after contract award.

(4) Breach Notification. The contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR) upon discovery of any suspected or confirmed breach in the security of NRC owned or controlled PII.

(5) Legal Demands for Information. If a legal demand is made for NRC owned or controlled PII (such as by subpoena), the contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR). After notification, the NRC will determine whether and to what extent to comply with the legal demand. The Contracting Officer will then notify the contractor in writing of the determination and such notice will indicate the extent of disclosure authorized, if any. The contractor may only release the information specifically demanded with the written permission of the NRC Contracting Officer.

(6) Audits. The NRC may audit the contractor's compliance with the requirements of this clause, including through the use of online compliance software.

(7) Flow-down. The prime contractor will flow this clause down to subcontractors that would be covered by any portion of this clause, as if they were the prime contractor.

(8) Remedies:

(a) The contractor is responsible for implementing and maintaining adequate security controls to prevent the loss of control or unauthorized disclosure of NRC owned or controlled PII in its possession. Furthermore, the contractor is responsible for reporting any known or suspected loss of control or unauthorized access to PII to the NRC in

accordance with the provisions set forth in Article 4 above.

(b) Should the contractor fail to meet its responsibilities under this clause, the NRC reserves the right to take appropriate steps to mitigate the contractor's violation of this clause. This may include, at the sole discretion of the NRC, termination of the subject contract.

(9) Indemnification. Notwithstanding any other remedies available to the NRC, the contractor will indemnify the NRC against all liability (including costs and fees) for any damages arising out of violations of this clause.

H.9 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS

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

H.10 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (SEP 2013)

Prior to occupying any Government provided space at NRC Headquarters 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, Office of Administration. 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

H.11 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES

(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.

H.12 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS

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.

H.13 NRC INFORMATION TECHNOLOGY SECURITY

NRC contractors shall ensure that their employees, consultants, and subcontractors with

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

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

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the NRC throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

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

H.14 SAFETY OF ON-SITE CONTRACTOR PERSONNEL

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

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

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

H.15 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS

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.

H.16 RULES OF BEHAVIOR FOR AUTHORIZED COMPUTER USE

In accordance with Appendix III, "Security of Federal Automated Information Resources," to Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," NRC has established rules of behavior for individual users who access all IT computing resources maintained and operated by the NRC or on behalf of the NRC. In response to the direction from OMB, NRC has issued the "Agency-wide Rules of Behavior for Authorized Computer Use" policy, hereafter referred to as the rules of behavior. The rules of behavior for authorized computer use will be provided to NRC computer users, including contractor personnel, as part of the annual computer security awareness course.

The rules of behavior apply to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC. This policy does not apply to licensees. The next revision of Management Directive 12.5, "NRC Cyber Security Program,"will include this policy. The rules of behavior can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The rules of behavior are effective immediately upon acknowledgement of them by the person who is informed of the requirements contained in those rules of behavior. All current contractor users are required to review and acknowledge the rules of behavior as part of the annual computer security awareness course completion. All new NRC contractor personnel will be required to acknowledge the rules of behavior within one week of commencing work under this contract and then acknowledge as current users thereafter. The acknowledgement statement can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB_Ack.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The NRC Computer Security Office will review and update the rules of behavior annually

beginning in FY 2011 by December 31st of each year. Contractors shall ensure that their personnel to which this requirement applies acknowledge the rules of behavior before beginning contract performance and, if the period of performance for the contract lasts more than one year, annually thereafter. Training on the meaning and purpose of the rules of behavior can be provided for contractors upon written request to the NRC Contracting Officer's Representative (COR).

The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order if such subcontracts/agreements will authorize access to NRC electronic and information technology (EIT) as that term is defined in FAR 2.101.

H.17 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS

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. 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.

H.18 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 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.

H.19 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 risked-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 risked-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.

H.20 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, NRC Cyber 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 12.5NRC Cyber 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

H.21 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (SEP 2013)

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.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, 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.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, 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.

H.22 NRC INFORMATION TECHNOLOGY SECURITY TRAINING

Agencies/Contractors shall ensure that their employees, consultants, and subcontractors with access to the NRC's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day. Agency/Contractor shall ensure that their employees, consultants, and subcontractors, with access to the NRC's IT equipment, complete the Information Security (INFOSec) Awareness Training annually; no later than December 31.

Agency/Contractor employees, consultants, and subcontractors shall complete the NRC's online, "Computer Security Awareness" course on the same day that they receive access to the NRC's IT equipment and/or services, as their first action using the equipment/service. For those Agency/Contractor employees, consultants, and subcontractors who are already working under an existing agreement/contract, the online training must be completed in accordance with agency Network Announcements issued throughout the year.

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

Agency/Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

The NRC reserves the right to deny or withdraw Agency/Contractor use or access to NRC IT equipment and/or services should the Agency/Contractor violate the Agency/Contractor's responsibility under this clause.

SECTION I - CONTRACT CLAUSES

I.2 52.227-17 RIGHTS IN DATA--SPECIAL WORKS. (DEC 2007)

(a) Definitions. As used in this clause--

Data means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

Unlimited rights means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of Rights. (1) The Government shall have--

(i) Unlimited rights in all data delivered under this contract, and in all data first produced in the performance of this contract, except as provided in paragraph (c) of this clause.

(ii) The right to limit assertion of copyright in data first produced in the performance of this contract, and to obtain assignment of copyright in that data, in accordance with paragraph (c)(1) of this clause.

(iii) The right to limit the release and use of certain data in accordance with paragraph (d) of this clause.

(2) The Contractor shall have, to the extent permission is granted in accordance with paragraph (c)(1) of this clause, the right to assert claim to copyright subsisting in data first produced in the performance of this contract.

(c) Copyright--(1) Data first produced in the performance of this contract. (i) The Contractor shall not assert or authorize others to assert any claim to copyright subsisting in any data first produced in the performance of this contract without prior written permission of the Contracting Officer. When copyright is asserted, the Contractor shall affix the appropriate copyright notice of 17 U.S.C. 401 or 402 and acknowledgment of Government sponsorship (including contract number) to the data when delivered to the Government, as well as when the data are published or deposited for registration as a published work in the U.S. Copyright Office. The Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license for all delivered data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

(ii) If the Government desires to obtain copyright in data first produced in the performance of this contract and permission has not been granted as set forth in paragraph (c)(1)(i) of this clause,

the Contracting Officer shall direct the Contractor to assign (with or without registration), or obtain the assignment of, the copyright to the Government or its designated assignee.

(2) Data not first produced in the performance of this contract. The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract and that contain the copyright notice of 17 U.S.C. 401 or 402, unless the Contractor identifies such data and grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause.

(d) Release and use restrictions. Except as otherwise specifically provided for in this contract, the Contractor shall not use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.

(e) Indemnity. The Contractor shall indemnify the Government and its officers, agents, and employees acting for the Government against any liability, including costs and expenses, incurred as the result of the violation of trade secrets, copyrights, or right of privacy or publicity, arising out of the creation, delivery, publication, or use of any data furnished under this contract; or any libelous or other unlawful matter contained in such data. The provisions of this paragraph do not apply unless the Government provides notice to the Contractor as soon as practicable of any claim or suit, affords the Contractor an opportunity under applicable laws, rules, or regulations to participate in the defense of the claim or suit, and obtains the Contractor's consent to the settlement of any claim or suit other than as required by final decree of a court of competent jurisdiction; and these provisions do not apply to material furnished to the Contractor by the Government and incorporated in data to which this clause applies.

SECTION J - LIST OF ATTACHMENTS

ATTACHMENT	TITLE
1	STATEMENT OF WORK
2	PRICE SCHEDULE
3	BILLING INSTRUCTIONS FIXED PRICE
4	BILLING INSTRUCTIONS LABOR HOUR

DELIVERY ORDER NRC-HQ-7S-14-T-0001

Computer Security Office (CSO)

General Support Services

1.0 OBJECTIVE

The Contractor shall support the Nuclear Regulatory Commission (NRC) in its efforts to develop and implement the organization's Information Security Program.

2.0 SCOPE OF WORK

The Contractor must ensure NRC's Information Security Program meets federally mandated and NRC defined security requirements. The Contractor shall provide the following services to the CSO:

- Provide Integrated Project Planning and Activity Scheduling
- Develop Supporting Documentation
- Provide Communications Support
- Support the Information Security Program
- Provide Security Engineering Support

The Contractor shall provide the necessary security support staff to meet the requirements specified in this Statement of Work (SOW).

3.0 TASKS

The Contractor shall support the organization according to the schedule of supplies, services, and prices found in the Consolidated Information Security Support Services (CISSS) contract as well as support the management and of active task orders under CISSS.

Note: At no time is the Contractor allowed to configure an NRC operational system.

Subtask 1: Provide Integrated Project Planning and Activity Scheduling

The project plan shall include an integrated Level 5 Work Breakdown Structure (WBS) across all task orders that have been defined under the contract. The WBS shall include a definition of the work to be conducted decomposed into distinct discrete manageable tasks or groups of tasks (work packages) with decisive outputs and specific measurable entry and exit criteria. Each work package shall be assigned a start and finish date, a budget value, and is integrated with the project plans from other task orders.

Also, the project plan shall provide resource utilization information that identifies the budget to accomplish the work, the resources needed to complete the work, and the effort required in the specified time frame for the completion of each of the tasks in the WBS. The Contractor shall allocate a portion of the budget for each work package that comprises the WBS and ensure that the WBS adequately defines all work necessary to meet the requirements for the project.

Microsoft Project Plan that incorporates all tasks and projects such that the individual projects roll up into an Integrated Security project schedule encompassing all NRC security related activities, services, and deliverables. The Microsoft Project Plan shall identify resources for each activity and include the Work Breakdown Structure levels.

Subtask 2: Develop Supporting Documentation

The Contractor shall develop documentation that supports the CSO's efforts to develop and implement a robust Information Security Program. Documentation will be used to ensure the security program meets enacted federal laws (Federal Information Security Management Act (FISMA), Privacy Act, etc.), federally mandated requirements (Office of Management and Budget (OMB), Code of Federal Regulations (CFR), Presidential Directives, etc.) and NRC defined security requirements. Also, the contractor shall assist the CSO in developing procedures, standards, and guidance that supports the organization's Security Policies.

The following describes some of the documentation the Contractor will have to develop under this subtask:

- New Security Policies (resulting from new technology, new attack methodologies, new federally mandated requirements)
- New Procedures (Continuous Monitoring Qtrly Scanning, FISMA Compliance Plans)
- Process Improvement Documentation
- New Standards (Windows 2003 or currently available Hardening Guidelines, Linux Hardening Guidelines)
- New Guidance (How the NRC intends to implement a new Presidential Directive, How the NRC intends to implement new technology, How a new policy should be implemented)

Subtask 3: Provide Communications Support

The Contractor shall provide communications support (briefings, demonstrations, etc.) when CSO is communicating with upper management or the user community. These activities will focus on assisting the CSO as it communicates NRC policy, standards, procedures, or security related requirements.

Subtask 4: Support Information Security Program

The Contractor shall support the CSO in the development, implementation, and continuous improvement of the agency's Information Security Program and ensure the risks/deficiencies in the program are being addressed in a timely and effective manner. An Information Security Program includes the following: security policies, incident handling, security training, capital planning, information system development life cycle, certification and accreditation, continuous monitoring, contingency planning, and system inventory.

The following identifies the support the contractor will provide under this subtask:

- The Contractor shall support the NRC's efforts to certify and accredit its information systems.

- The Contractor shall support the NRC's efforts to establish a contingency planning process that addresses the needs of the agency.
- The Contractor shall support the NRC staff in the development and documentation of security controls and security requirements and associated technical resolutions, risk mitigation, and implementations.
- The Contractor shall review, verify, and validate all security controls and security requirements and associated technical resolutions, risk mitigation, and implementations contained within various NRC security and systems development documentation such that confirmation that the system and associated controls are operating as intended.
- The Contractor shall perform quarterly analysis, penetration, vulnerability, configuration, systems integrity, and patch management scans. The Contractor shall identify, analyze, and propose tested corrective actions that ensure the agency's security posture is up to date and the security controls are operating as intended.
- The Contractor shall support the functional alignment of common security control sets and standard operating procedures consistent with FISMA and NIST SP 800-53 that integrates with the NRC's Project Management Methodology.
- Support the NRC in the development of a security line of business program and support the agency in assessing, documenting, and implementing common security solutions.
- The Contractor shall provide support to assist the CSO in meeting its FISMA reporting requirements and responding to Data Calls by the Office of Inspector General (OIG) and other government agencies.
- The Contractor shall provide technical support services to develop, implement, administer, and maintain the information systems tools that support the NRC's Information Security Program.

Subtask 5: Provide Security Engineering Support

The Contractor shall provide Security Engineering support to verify and validate that proposed architectures and implementations are based on sound security engineering principles and practices. The Contractor shall ensure that all federally mandated and NRC defined security requirements are met.

Subtask 6: Special Projects

The Computer Security Office (CSO) will need the following support services to ensure a robust information security program is developed and implemented at the NRC:

- Software Quality Assurance:

  The contractor will assist the CSO in developing a Software Quality Assurance Program that gives the NRC the capability to scan customized source code and object files for vulnerabilities and deficiencies. Under this program two types the following will be established:

  1. Developer Verification - Auditing software will be put in the hands of the developers so flaws and inadequacies that exist in their source code can be identified, prioritized, and understood. This will allow the developer to fix their source code immediately ensuring only hardened source code is used in NRC systems.
  2. CSO Verification - A service will be used to independently verify and validate that submitted source code has been properly hardened. This review will not only examine the developer's source code but any third party applications or libraries that are in use. This review should be done after major milestones have been accomplished.

  By utilizing these methods, the NRC will be able to develop a Software Quality Assurance Program that is robust and ensure customized source code is properly protected from attackers.

- Residual Risks:

  The contractor will develop and implement a process for determining the residual risk that exists in the NRC infrastructure. The contractor should focus on risks that occur at an enterprise level or impact multiple NRC information systems. Also, the contractor will develop a reporting template (Quarterly Residual Risk Report) and will brief the Computer Information Security Officer (CISO) and Director of Office of Information Systems (OIS) on a quarterly basis. [redacted]

  The contractor will use the following sources to determine these risks: audits, the Enterprise Risk Assessment, computer security incidents, Strategic Plan, Inspector General Reports, Plan of Action & Milestone items, vendor reported vulnerabilities & exploits, and observations. The contractor will identify and prioritize these risks and will map these risks to business needs and objectives.

  During the quarterly presentation, the contractor will identify new risks, all risks that have been closed in a quarter, and the top twenty risks that exist in the NRC. The contractor should provide options on how all risks identified in the Quarterly Residual Risk Report could be mitigated.

- Web Application Assessments:

  The contractor shall develop and implement a process to conduct Web Application Assessments at the NRC using Cenezic's Hailstorm Professional. The contractor will install Hailstorm Professional on three scanning laptops, develop procedures for configuring & executing an assessment, work with the CSO & OIS to test Hailstorm Professional in NRC's Consolidated Testing Facility, and work with CISSS scanning team to ensure assessments of productions web applications can be performed effectively and safely. [redacted]

• The configuration of the dedicated server and dedicated laptop analyzing the traffic of interest must meet NRC configuration standards and must be independently assessed by the NRC to determine compliance. Analysis will not begin until this is accomplished.

• All communications between the server and laptop used to analyze traffic must be protected using NIST FIPS 140-2 (level 2) validated encryption.

• Only cleared personnel will be allowed to install, operate, or maintain the hardware and software used to support this effort.

• All outbound traffic that is captured and unencrypted (no longer public) must be protecte using NIST FIPS 140-2 (level 2) validated encryption at all times (including at rest).

• All configuration changes to the dedicated server and dedicated laptop analyzing the tra of interest must be approved by the NRC prior to change implementation. The NRC Proje Officers will provide a list of changes that do not require NRC approval.

• The Contractor will notify the NRC immediately if any serious or catastrophic risk or vulnerability is detected.

• The NRC reserves the right to determine how all security incidents are handled.

[redacted]

• The Contractor will participate in Bi-weekly conference calls to discuss task status with the Project Officer, alternate Project Officer, and task sponsors.

• The Contractor will submit Monthly Technical Reports summarizing activities that have occurred on the task within the last 30 days. The Monthly Technical Reports must be delivered to the NRC Project Officer and Alternate Project Officer no later than the 5th working day of each month. The Contractor will meet with the NRC in person to discuss these reports.

• The Contractor will provide the NRC with a Formal Management Report that describes all threats and risks seen each quarter. The Formal Management Report is due to the NRC Project Officer and Alternate Project Officer no later than the is" business day of the following quarter. The Contractor will meet with the NRC in person to discuss these reports.

• The Contractor will provide and the NRC will host the tap and the device that collects traffic of interest. The Contractor will host at their facilities the dedicated server and dedicated laptop that analyzes the traffic of interest. All analysis of suspicious traffic will be performed on this dedicated equipment.

Subtask 7: Red Team Penetration Testing

The Contractor shall conduct external penetration tests and social engineering tests against the NRC infrastructure. The Contractor shall use a variety of testing tools, manual and automatic, including proprietary and modified open source, to attempt to penetrate NRC systems.

In order to conduct this testing, the Contractor shall procure, lease, or otherwise obtain the commercially available tools needed to complete the testing. A designated government official must be present during all active penetration testing activities. Before testing commences, the contractor will submit a test plan that describes the effort in detail.

The NRC must approve the test plan and all tools used during the assessment in writing before testing begins. During testing, all sensitive NRC data (e.g., Sensitive Unclassified Non-Safeguards Information) must be encrypted using NIST FIPS 140-2 validated encryption while in transit. All NRC data related to testing must be encrypted using NIST FIPS 140-2 validated encryption while at rest.

The NRC's use of its domain space includes both internal as well as external trusted information services providers.

The Contractor will not conduct any testing until they have received written approval in an authorized and completed Rules of Engagement document from the NRC. The Contractor shall inform the Project Officers and the CSA SITSO before each activity that actively accesses NRC IT or parties operating IT resources on behalf of the NRC is conducted as part of this test. The Project Officers and the CSA SITSO do not need to be notified for activities that do not actively access NRC IT resources or parties operating IT resources on behalf of the NRC.

Penetration Testing Phases

The contractor may use company processes and techniques that enhance or provide a best practices red team penetration test environment for this sub task; however at a minimum, the following phases and / or steps shall be included as part of the testing engagement:

Phase 1 – Planning, Preparation and Authorization -

- **Step 1 –Identify Penetration Test Tools and Proposed Test Plan**– The contractor shall develop a Tools and Proposed Red Team Test Plan that identifies the automated tools that are going to be used for this sub task. At a minimum, the test plan will identify the analysts who will conduct red team testing, the testing tools that will be used, the tests that will be run during the discovery and penetration testing phase, the time windows (dates) for the discovery and testing phases, the physical and Internet Protocol addresses that will be used to conduct the tests and the potential impact on NRC IT systems as a result of testing.

- **Step 2 - Complete and Receive an NRC Authorized Rules of Engagement Agreement** – The contractor will complete a Rules of Engagement Document for this sub task that follows the format and security principles outlined in the National Standard of Institute's Special Publication 800-115, Technical Guide to Information Security Testing and Assessment as applicable for external penetration test. An ROE template example which may be modified as necessary to execute this Sub Task is attached as Appendix A.

- **Phase 2 – Discovery**
  - **Information Gathering** – The contractor shall gather information through fingerprinting and mapping of the *.nrc.gov domain space using information available via the Internet such as, but not limited to DNS, who-is, agency information available through internet search engines and social engineering, and network mapping and topology generated from the discovery phase to identify the touch points that need to be tested (for example: Routers, Firewalls, Gateways, Remote Access Services, Web Applications, Adherence to policies & standards, etc.). The Contractor will provide the NRC with the complete information gathered during the discovery phase and will prioritize the testing of this list after consultation with the NRC CSA SITSO and the Project Officers.

- **Phase 3 - Testing** - The contractor will perform external penetration testing and social engineering attacks against the NRC under observation by a designated government official. All raw scans, observations, and testing results will be captured and documented in the corrective action report.

Monthly Report

The Contractor shall provide a Monthly Performance Report that provides status of work accomplished, work forecast, and any concerns or potential problem areas. The format of the Monthly Performance Report must be agreed upon before work under this sub task may begin. The Monthly Performance Report will be provided on the 5th of every month in Microsoft Word Version 2007 format (a later version may be used with the approval of the NRC).

- **Phase 4 - Red Team Report and Presentation** –

The Contractor will develop a draft and final report and a presentation designed for department heads and other senior executives that summarize the findings of the Red Team Penetration Test, identifying the current risks to NRC sensitive information and the information systems that exhibit these risks.

The report and presentation should be developed in a format readable by Microsoft Office Word and PowerPoint Version 2007 (a later version may be used with the approval of the NRC). The NRC will have five business days to review and comment on the draft documents. The contractor, upon receiving the NRC comments, will have five additional business days to incorporate agency comments and provide final documents reports to the Director, OIS, the Chief Information Security Officer, the CSA SITSO and the Project Officers.

- The Red Team Report and Presentation shall contain but shall not be limited to addressing the following areas:
    - Summarize how the tests were performed and how risk was evaluated.
    - Identify the tool and type of test that was run (e.g.; Nessus, Backtrack, fingerprinting SQL injection, etc.)
    - Specify the IP addresses, hostnames and users that were tested and the information systems/organizations that the tested components form as a system configuration item (to the extent that the information is available or can be derived to make an assignment).
    - Describe the vulnerabilities and deficiencies that were discovered during testing.
    - Identify the risks associated with these vulnerabilities and deficiencies. Risks will be organized with the most significant risk listed first.
    - Provide recommendations on how to mitigate these risks. A recommendation will be provided for every risk.

- **Phase 5: Cleanup** – The contractor shall wipe all devices used during testing and certify in writing that the task was completed using Department of Defense (DoD) approved sanitization methods. All contractors associated with this sub task will sign non-disclosure agreements and not publish, discuss or otherwise communicate the test findings to individuals outside the NRC without rewritten authorization by the Government.

Schedule

The contractor shall provide a project schedule for all tasks, monthly reports, draft and final reports identified within this sub task to be completed not later than 80 days from award. With the exception of the deliverable identified in Section 3.2 of this sub task, one copy of each deliverable shall be provided as required electronically to the NRC CSA SITSO or his designee. All report formats not identified in this sub task must be agreed to by the NRC before the reports are delivered. Deliverables shall be considered accepted by NRC if no edits have been sent to Contractor dated within five business days of receipt.

Personnel

The Contractor shall assign a single individual to serve as the primary point of contact and project manager to support this sub task. All Contractor personnel will be knowledgeable in one or more disciplines directly related to information. All personnel working on this sub task must be pre-approved by the NRC.

Access to classified information is required. Since information protection is a very sensitive issue, Contractor personnel must have an approved background check that corresponds to the NRC information they need access too. It is anticipated that the Contractor will need an NRC "L" clearance.

Subtask 8: Automated Compliance

The phases for the initiative are

a. Phase 1 –Contractor will conduct a Best Practice/Configuration Review of the NRC's nCircle implementation and will provide configuration changes that should be made to more effectively use the tool.

b. Phase 2 – Contractor will develop two (2) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.

c. Phase 3 – Contractor will develop six (6) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.

d. Phase 4 – Contractor will develop six (6) templates that can be utilized with the NRC's nCircle implementation to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements.

Phase Detail

The following describe each phase and identifies the services that the contractor is expected to provide.

Phase 1 – Perform Best Practices/Configuration Review **(Optional)**

The Best Practices/Configuration Review includes the contractor's investigation of the implementation of the nCircle within the NRC environment, covering specific aspects of the configuration, reporting, management processes, and maintenance of the nCircle suite of tools. The review will investigate NRC's deployment from two major perspectives:

- Technology — the configuration of the software itself.
- Processes and Workflow — the scanning, reporting, and remediation lifecycle.

Technology

The contractor will use a combination of hands-on investigation, reviews of available process documentation, and interviews with key stakeholders to conduct the review. The contractor will carefully manage the level of detail to ensure all topics are addressed at least at a high level. The following are the standard topic areas that will be included in this review:

Topic Area	Task	Description
Configuration Auditing Program	Configuration Auditing Goals	Review NRC's goals and expectations for configuration auditing.
Operations	Ticket Review	Review status and resolution of all nCircle support tickets since the last tune up.
	Operational Issues	Review any outstanding issues as noted by NRC staff.
Architecture	Architecture Review	Review deployment of scan engines, management servers, and SQL databases and compare against best practices; suggest improvements as needed.
Network Profiles	Naming Conventions	Review naming conventions and structure for network profiles, asset groups, and meta-asset groups and compare to best practices; determine optimal settings for nCircle's Intelligence Hub if in use.
Asset Licensing	License Cleanup	Review licensed assets and recommend the removal of invalid or obsolete assets to free up license capacity.
Auto Grouping	Auto Group Configuration	Review configuration of auto-grouping and recommended improvements as needed.
Custom Properties	Custom Property Creation	Review custom properties against business needs and recommend improvements.

Topic Area	Task	Description
Port Profiles	Port Profile Configuration	Review port profiles in use and recommend ways to optimize discovery and performance.
Risk Levels	Risk Level Configuration	Review assigned risk levels and ensure they map to business needs.
Scan Credentials	Credentials Configuration	Review structure and use of credentials for scanning and compare to best practices.
Scan Engines	DNS Server Configuration	Review DNS settings and validate domain name resolution functionality.

Security	Audit Log Configuration	Review NRC's audit requirements and compare against audit log settings.
User Management	User and Roles Review	Review configuration of the nCircle users and roles, and the permissions granted; compare to best practices.
Software Upgrades	Current Version Installation	Review any issues or improvements delivered by newer versions of the nCircle product.
System Health	Health Events	Review any system health events.
Third Party Integration	Third Party Configuration	Review configuration of Checkpoint, NAC, HP CMDB, Remedy, and Vulnerability Scanner settings.
Scan Configuration	Discovery Ping Sweep Configuration	Review configuration of discovery ping sweeps including TCP SYN, ARP, etc. and compare against best practices.
	Port Scan Configuration	Review configuration of port scans including banner checking, OS socket usage, NMAP fingerprints, etc. and compare against best practices.
	Advanced Scan Configuration	Review configuration of advanced scan categories, including Antivirus settings, file monitoring for both Windows and UNIX, Oracle database instance configuration, Users configuration, etc. and compare against NRC's needs and best practices.
	Gather Host Information Configuration	Review configuration of host information gathering, including fingerprinting, NetBIOS probes, and DNS settings and compare against best practices.
	Web Content Scan Configuration	Review configuration of web content scanning, including paths, crawling, ports, and page depth, and compare against best practices.
Dashboard	Dashboard Configuration	Review configuration and operation of the nCircle's dashboard; validate settings and test NRC's implementation of the dashboard.
Compliance Policies	Compliance Policy Configuration	Review usage of nCircle policies and compare to best practice; suggest improvements or additional scanning based on typical peer group configurations.

Topic Area	Task	Description
	Custom Test Usage	Review design and functionality of custom tests implemented at the NRC.
	Create Policy From Asset Usage	Review NRC use of "Create Policy from Asset" capabilities; assist with the creation of policies from Gold image systems as required.
Reports	Report Usage	Review NRC use of nCircle reports and compare to best practices.
Integration	External System Integration Proposals	Review capabilities for integration with external systems (ArcSight, Remedy, etc.)
Roadmap	Roadmap Presentation	Discuss future capabilities and estimated timeframes for future versions of the nCircle.
	Feature Requests	Document NRC feature requests and submit tickets for tracking and follow up.
Operations	Best Practice Recommendations	Review findings and provide documentation detailing what needs to be done.
Overall Tool Configuration	Assess the overall tool configuration	Determine if any tool configuration changes could be made to improve tool effectiveness

As the contractor identifies quick fix recommendations during the review, the contractor will document these changes and provide them to NRC. Most of the quick fix recommendations will fall into the category of tuning, i.e. adjustments to the nCircle configuration parameters that can be implemented very quickly. There will likely be other needed changes identified that will be longer range in scope, especially if these entail modifications to NRC's current processes and workflow.

Processes and Workflow

The contractor will review NRC's processes and workflow surrounding NRC's use of the nCircle and other tools that might be involved in remediation of vulnerabilities and compliance issues. This investigation covers key questions such as:

- Are current nCircle processes understood and followed?
- Will current nCircle processes be able to scale as the nCircle implementation is extended to other network segments and to include additional templates?
- What other impediments exist to achieving full nCircle deployment and how can these be mitigated?
- Is there significant manual effort that could be addressed through increased automation?

During the review, the contractor will work with NRC staff directly responsible for the day-to-day administration and management of the nCircle, to provide focused knowledge transfer on topics of interest or concern to NRC. During this knowledge transfer, the contractor will demonstrate and explore key concepts in the nCircle allowing for technical Q&A from NRC staff.

The contractor will conduct a technical debrief for NRC staff, covering the major findings and recommendations arising from the Best Practices/Configuration Review for the nCircle implementation. The contractor will discuss the modifications and optimization recommendations interactively with NRC.

The contractor will document all review findings and recommendations and will provide these to NRC in a narrative document, covering all the topic areas addressed during the review.

List of Deliverables

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Findings and Recommendations Report	Narrative document covering topic areas addressed during the configuration review and associated recommendations

Completion Criteria

The contractor will have fulfilled all of their responsibilities under this task upon NRC's acceptance of a final Findings and Recommendations Report.

Schedule and Work Location

The contractor will perform the review during a single visit to the NRC's offices in Rockville, MD. The schedule for the on-site portion of the review will be confirmed by mutual agreement between the contractor and NRC.

NRC Responsibilities

In order for the contractor to successfully perform the Services described in this task, the contractor requests the following from NRC:

1. Provide a conference room for meetings between the contractor staff and NRC staff
2. Provide adequate workspace facilities for contractor staff while working on site
3. Provide access to test and/or production implementations of nCircle.
4. Assign and engage review participants (subject matter experts) to work with the contractor to provide requirements and validate finding
5. Ensure some review participants are familiar with NRC's specific implementation of nCircle and can provide detailed technical information about NRC's current implementation of the tool and the networks being scanned.

Phase 2 – Develop two (2) nCircle Templates (Optional)

The contractor will develop two (2) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop two (2) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

Phase 3 – Develop six (6) nCircle Templates (Optional)

The contractor will develop six (6) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

Phase 4 – Develop six (6) nCircle Templates (Optional)

The contractor will develop six (6) nCircle Templates that will be used in conjunction with the nCircle tool to assess NRC information technology resources in an automated fashion ensuring the resources address federally mandated and NRC defined cyber security requirements. NRC will provide the NRC defined cyber security requirements that must be incorporated into the nCircle templates.

The templates developed by the contractor must be approved by the NRC before they are considered complete.

The contractor will provide the following Deliverable(s) to NRC during this phase:

DELIVERABLE	DESCRIPTION
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.
Develop six (6) nCircle templates that reflect NRC defined cyber security requirements	Templates that work with NRC's implementation of nCircle to assess implementation compliance against NRC specific cyber security requirements.

5.0 TRAVEL

Travel may be required for this effort and should not exceed $20K per year.

6.0 MEETINGS

As needed, the Contractor's Project Manager and technical lead shall attend status meetings at NRC Headquarters to discuss issues and work being performed under this task order.

NRC-HQ-11-14-T-0002 Price Schedule			
Labor Category	**Labor Rate**	**Hours**	**Cost**
Program Manager	$153.98	100	$15,398.00
Project Manager	$138.09	960	$132,566.40
Computer Forensic and Intrusion Analyst	$252.56	100	$25,256.00
Sr. Cyber Security Consultant	$241.95	100	$24,195.00
Senior INFOSEC Engineer	$209.86	400	$83,944.00
Security Specialist IV	$163.59	5640	$922,647.60
Security Specialist III	$144.47	100	$14,447.00
Security Specialist II	$138.09	2200	$303,798.00
Security Specialist I	$116.09	100	$11,609.00
Documentation Specialist	$91.22	2200	$200,684.00
Information Engineer	$85.28	200	$17,056.00
Technical Writer II	$67.33	1880	$126,580.40
Technical Writer I	$44.39	960	$42,614.40
		LABOR TOTAL	**$1,920,795.80**
		NTE TRAVEL TOTAL	**$20,000.00**
		GRAND TOTAL	**$1,940,795.80**

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

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

The contractor shall prepare invoices/vouchers for reimbursement of costs in the manner and format described herein. FAILURE TO SUBMIT INVOICES/VOUCHERS IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE INVOICE/VOUCHER AS IMPROPER.

Standard Forms: Claims shall be submitted on the payee's letterhead, invoice/voucher, 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."

Electronic Invoice/Voucher Submissions: The preferred method of submitting vouchers/invoices is electronically to the U.S. Nuclear Regulatory Commission, via email to: NRCPayments@nrc.gov.

Hard-Copy Invoice/Voucher Submissions: If you submit a hard-copy of the invoice/voucher, a signed original and supporting documentation shall be submitted to the following address:

NRC Payments
U.S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike
Mailstop O3-E17A
Rockville, MD 20852-2738

Purchase of Capital Property: *($50,000 or more with life of one year or longer)*

Contractors must report to the Contracting Officer, electronically, any capital property acquired with contract funds having an initial cost of $50,000 or more, in accordance with procedures set forth in NRC Management Directive (MD) 13.1, IV, C – "Reporting Requirements" (revised 2/16/2011).

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

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

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

Format: Invoices/Vouchers shall be submitted in the format depicted on the attached sample form entitled "Invoice/Voucher for Purchases and Services Other Than Personal". Alternate formats are permissible only if they address all requirements of the Billing Instructions. The instructions for preparation and itemization of the invoice/voucher are included with the sample form.

Task Order Contracts: The contractor must submit a separate invoice/voucher for each individual task order with detailed cost information. This includes all applicable cost elements and other items discussed in paragraphs (a) through (q) of the attached instructions. In addition, the invoice/voucher must specify the contract number, and the NRC-assigned task/delivery order number.

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

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

Currency: Invoices/Vouchers must be expressed in U.S. Dollars.

Supersession: These instructions supersede previous Billing Instructions for Time-and-Materials/Labor-Hour Type Contracts (July 2011).

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL (SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

NRC Payments
U.S. Nuclear Regulatory Commission
One White Flint North
11555 Rockville Pike
Mailstop O3-E17A
Rockville, MD 20852-2738

2. Invoice/Voucher Information

a. Payee's DUNS Number or DUNS+4. The Payee shall include the Payee's Data Universal Number (DUNS) or DUNS+4 number that identifies the Payee's name and address. The DUNS+4 number is the DUNS number plus a 4-character suffix that may be assigned at the discretion of the Payee to identify alternative Electronic Funds Transfer (EFT) accounts for the same parent concern.

b. Payee's Name and Address. Show the name of the Payee as it appears in the contract and its correct address. If the Payee assigns the proceeds of this contract as provided for in the assignment of claims terms of this contract, the Payee shall require as a condition of any such assignment, that the assignee shall register separately in the System for Award Management (SAM) database at http://sam.gov and shall be paid by EFT in accordance with the terms of this contract. See Federal Acquisition Regulation (FAR) 52.232-33(g) Payment by Electronic Funds Transfer - Central Contractor Registration (October 2003).

c. Taxpayer Identification Number. The Payee shall include the Payee's taxpayer identification number (TIN) used by the Internal Revenue Service (IRS) in the administration of tax laws. (See IRS Web site: http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Employer-ID-Numbers-(EINs)).

d. Contract Number. Insert the NRC contract number (including Enterprise-wide Contract (EWC)), GSA Federal Supply Schedule (FSS), Governmentwide Agency Contract (GWAC) number, or Multiple Agency Contract (MAC) number, as applicable.

e. Task Order Number. Insert the task/delivery order number (If Applicable). **Do not include more than one task order per invoice or the invoice may be rejected as improper.**

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

f. Invoice/Voucher. The appropriate sequential number of the invoice/voucher, beginning with 001 should be designated. Contractors may also include an individual internal accounting number, if desired, in addition to the 3-digit sequential number.

g. Date of Invoice/Voucher. Insert the date the invoice/voucher is prepared.

h. Billing period. Insert the beginning and ending dates (day, month, year) of the period during which costs were incurred and for which reimbursement is requested.

i. Labor Hours Expended. Provide a general summary description of the services performed and associated labor hours utilized during the invoice period. Specify the Contract Line Item Number (CLIN) or SubCLIN, as applicable, and information pertaining to the contract's labor categories/positions, and corresponding authorized hours.

j. Property. For contractor acquired property, list each item with an initial acquisition cost of $50,000 or more and provide: (1) an item description, (2) manufacturer, (3) model number, (4) serial number, (5) acquisition cost, (6) date of purchase, and (7) a copy of the purchasing document.

k. Shipping. Insert weight and zone of shipment, if shipped by parcel post.

l. Charges for freight or express shipments. Attach prepaid bill if shipped by freight or express.

m. Instructions. Include instructions to consignee to notify the Contracting Officer of receipt of shipment.

n. For Indefinite Delivery contracts, the final invoice/voucher shall be marked "FINAL INVOICE" or "FINAL VOUCHER".

o. Direct Costs. Insert the amount billed for the following cost elements, adjustments, suspensions, and total amounts, for both the current billing period and for the cumulative period (from contract inception to end date of this billing period).

(1) Direct (Burdened) Labor. This consists of salaries and wages paid (or accrued) for direct performance of the contract itemized, including a burden (or load) for indirect costs (i.e., fringe, overhead, General and Administrative, as applicable), and profit component, as follows:

Labor Category	Hours Billed	Burdened Hourly Rate	Total	Cumulative Hours Billed

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

(2) Contractor-acquired property ($50,000 or more). List each item costing $50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) an item description, (b) manufacturer, (c) model number, (d) serial number, (e) acquisition cost, (f) date of purchase, and (g) a copy of the purchasing document.

(3) Contractor-acquired property (under $50,000), Materials, and Supplies. These are equipment other than that described in (2) above, plus consumable materials and supplies. List by category. List items valued at $1,000 or more separately. Provide the item number for each piece of equipment valued at $1,000 or more.

(4) Materials Handling Fee. Indirect costs allocated to direct materials in accordance the contractor's usual accounting procedures.

(5) Consultant Fee. The supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval (if not specifically approved in the original contract).

(6) Travel. Total costs associated with each trip must be shown in the following format:

Start Date		Destination		Costs
From	To	From	To	$

(Must include separate detailed costs for airfare, per diem, and other transportation expenses. All costs must be adequately supported by copies of receipts or other documentation.)

(7) Subcontracts. Include separate detailed breakdown of all costs paid to approved subcontractors during the billing period.

p. Total Amount Billed. Insert columns for total amounts for the current and cumulative periods.

q. Adjustments. Insert columns for any adjustments, including outstanding suspensions for unsupported or unauthorized hours or costs, for the current and cumulative periods.

r. Grand Totals.

ATTACHMENT

BILLING INSTRUCTIONS FOR
TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

3. Sample Invoice/Voucher Information

Sample Invoice/Voucher Information (Supporting Documentation must be attached)

This invoice/voucher represents reimbursable costs for the billing period from_____through_____.

			Amount Billed Current Period	Amount Billed Cumulative
(a)	**Direct Costs**			
	(1)	Direct burdened labor	$_____	$_____
	(2)	Government property ($50,000 or more)	$_____	$_____
	(3)	Government property, Materials, and Supplies (under $50,000 per item)	$_____	$_____
	(4)	Materials Handling Fee	$_____	$_____
	(5)	Consultants Fee	$_____	$_____
	(6)	Travel	$_____	$_____
	(7)	Subcontracts	$_____	$_____
		Total Direct Costs:	**$**_____	**$**_____
(b)	**Total Amount Billed**		**$**_____	**$**_____
(c)	**Adjustments** (+/-)		**$**_____	**$**_____
(d)	**Grand Total**		**$**_____	**$**_____

(The invoice/voucher format provided above must include information similar to that included below in the following to ensure accuracy and completeness.)

SAMPLE SUPPORTING INFORMATION

The budget information provided below is for format purposes only and is illustrative.

Cost Elements:

1) Direct Burdened Labor - $4,800

Labor Category	Hours Billed	Burdened Rate	Total	Cumulative Hours Billed

ATTACHMENT

BILLING INSTRUCTIONS FOR TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

Senior Engineer I	100	$28.00	$2,800	975
Engineer	50	$20.00	$1,000	465
Computer Analyst	100	$10.00	$1,000	320
			$4,800	1,760 hrs.

Burdened labor rates must come directly from the contract.

2) Government-furnished and contractor-acquired property ($50,000 or more) - $60,000

Prototype Spectrometer - item number 1000-01 = $60,000

3) Government-furnished and contractor-acquired property (under $50,000), Materials, and Supplies - $2,000

10 Radon tubes @ $110.00	= $1,100
6 Pairs Electrostatic gloves @ $150.00	= $ 900
	$2,000

4) Materials Handling Fee - $40

(2% of $2,000 in item #3)

5) Consultants' Fee - $100

Dr. Carney - 1 hour fully-burdened @ $100 = $100

6) Travel - $2,640

(i) Airfare: (2 Roundtrip trips for 1 person @ $300 per r/t ticket)

Start Date	End Date	Days	From	To	Cost
4/1/2011	4/7/2011	7	Philadelphia, PA	Wash, D.C.	$300
7/1/2011	7/8/2011	8	Philadelphia, PA	Wash, D.C.	$300

(ii) Per Diem: $136/day x 15 days = $2,040

7) Subcontracting - $30,000

Company A	= $10,000
Company B	= $20,000
	$30,000

(EX: Subcontracts for Companies A & B were consented to by the Contracting Officer by letter dated 6/15/2011.)

ATTACHMENT

BILLING INSTRUCTIONS FOR
TIME-AND-MATERIALS/LABOR-HOUR TYPE CONTRACTS (MAY 2013)

Total Amount Billed	$99,580
Adjustments (+/-)	- 0
Grand Total	$99,580

4. Definitions

Material handling costs. When included as part of material costs, material handling costs shall include only costs clearly excluded from the labor-hour rate. Material handling costs may include all appropriate indirect costs allocated to direct materials in accordance with the contractor's usual accounting procedures.