ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES: 1 of 37

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

1. DATE OF ORDER: 02/26/2014	2. CONTRACT NO. (If any): GS06F0641Z
3. ORDER NO.: NRC-HQ-60-14-T-0001	4. REQUISITION/REFERENCE NO.: CSO-14-0002

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: ROCKVILLE | d. STATE: MD | e. ZIP CODE: 20852

7. TO: DANIEL HACKENBERG
a. NAME OF CONTRACTOR: MAR INCORPORATED
b. COMPANY NAME:
c. STREET ADDRESS: 1803 RESEARCH BOULEVARD
SUITE 204
d. CITY: ROCKVILLE | e. STATE: MD | f. ZIP CODE: 208506106

f. SHIP VIA:

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: OFF OF NUCLEAR REG RESEARCH

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		02/20/2015	

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: 02/26/2014 to 05/20/2022 Continued ...					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT:
19. GROSS SHIPPING WEIGHT:
20. INVOICE NO.:

21. MAIL INVOICE TO:
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: ROCKVILLE | d. STATE: MD | e. ZIP CODE: 20852-2738

17(h) TOTAL (Cont. pages): $71,348.28

17(i) GRAND TOTAL: $1,144,172.23

22. UNITED STATES OF AMERICA BY (Signature): 02/26/2014 Joseph L. Widdup

23. NAME (Typed): JOSEPH L. WIDDUP
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (Rev. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.212

TEMPLATE - ADM001

SUNSI REVIEW COMPLETE

APR 10 2014

ADM002

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
02/26/2014	GS06F0641Z	NRC-HQ-60-14-T-0001

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
00001	Base Year Contractor Labor-Hours - See Attachment 2 for authorized labor categories and fixed hourly rates. Line Item Ceiling$71,348.28 Incrementally Funded Amount: $1,000.00				71,348.28	
00002	Fixed Price items. See Attachment 2 Price Schedule for listing of Fixed Price items. Amount: $65,874.69(Option Line Item) Anticipated Excercise Date01/20/2016 Line Item Ceiling$65,874.69 Incrementally Funded Amount: $0.00				0.00	
10001	Option Year 1 Amount: $137,222.97(Option Line Item) Anticipated Excercise Date01/20/2015				0.00	
20001	Option Year 2 Amount: $137,935.76(Option Line Item) Anticipated Excercise Date01/20/2016				0.00	
30001	Option Year 3 Amount: $137,935.76(Option Line Item) Anticipated Excercise Date01/20/2017				0.00	
40001	Option Year 4 Amount: $138,655.85(Option Line Item) Anticipated Excercise Date01/20/2018				0.00	
50001	Option Year 5 Amount: $138,655.85(Option Line Item) Anticipated Excercise Date01/20/2019				0.00	
60001	Option Year 6 Amount: $138,655.85(Option Line Item) Anticipated Excercise Date01/20/2020				0.00	
70001	Option Year 7 Amount: $138,655.85(Option Line Item) Anticipated Excercise Date01/20/2021				0.00	
80001	Option Year 8 Amount: $39,231.37(Option Line Item) Continued ...				0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) ▷ $71,348.28

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

DATE OF ORDER	CONTRACT NO	ORDER NO.
02/26/2014	GS06F0641Z	NRC-HQ-60-14-T-0001

ITEM NO (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Anticipated Excercise Date01/20/2022 The obligated amount of award: $1,000.00. The total for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $0.00

Contents

SECTION B - SUPPLIES OR SERVICES/PRICES

B.1 CONSIDERATION AND OBLIGATION -TASK ORDERS

(a) The ceiling of this order for the services is **$137,222.97**.

Option 1 (if exercised) is priced at $137,222.97.

Option 2 (if exercised) is priced at $137,935.76.

Option 3 (if exercised) is priced at $137,935.76.

Option 4 (if exercised) is priced at $138,655.85.

Option 5 (if exercised) is priced at $138,655.85.

Option 6 (if exercised) is priced at $138,655.85.

Option 7(if exercised) is priced at $138,655.85.

Option 8 (if exercised) is priced at $39,231.37.

(b) This order is subject to the minimum and maximum ordering requirements set forth in the contract GS06F0641Z.

(c) The amount presently obligated with respect to this order is **$1,000.00**. 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 – CSPSS Statement of Work

SECTION F - DELIVERIES OR PERFORMANCE

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

This order shall commence on February 21, 2014 and will expire on February 20, 2015.

Option Period 1 (if exercised) will be February 21, 2015 through February 20, 2016.

Option Period 2 (if exercised) will be February 21, 2016 through February 20, 2017.

Option Period 3 (if exercised) will be February 21, 2017 through February 20, 2018.

Option Period 4 (if exercised) will be February 21, 2018 through February 20, 2019.

Option Period 5 (if exercised) will be February 21, 2019 through February 20, 2020.

Option Period 6 (if exercised) will be February 21, 2020 through February 20, 2021.

Option Period 7 (if exercised) will be February 21, 2021 through February 20, 2022.

Option Period 8 (if exercised) will be February 21, 2022 through May 20, 2022.

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:	Shane Rupinta
Address:	Two White Flint North, Mail Stop: CSB/C6 D20 11545 Rockville Pike Rockville, MD 20852-2738
Telephone Number:	301-251-7992
Email:	shane.rupinta@nrc.gov

Alternate Contracting Officer's Representatives:

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

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, contract change, claim, or dispute.

H.6 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS

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

H.7 GREEN PURCHASING (SEP 2013)

(a) In furtherance of the sustainable acquisition goals included in Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," products and services acquired under this contract/order shall be energy-efficient (Energy Star or Federal Energy Management Program (FEMP) designated), water-efficient, biobased, environmentally preferable (e.g., Electronic Product Environmental Assessment Tool (EPEAT) certified), non-ozone depleting, recycled content, and non-toxic or less toxic alternatives, to the maximum extent practicable in meeting NRC contractual requirements.

(b) See NRC's Green Purchasing Plan (GPP) at: http://pbadupws.nrc.gov/docs/ML1219//ML12191A130.pdf and the General Service Administration's (GSA) Green Procurement Compilation at: http://www.gsa.gov/portal/content/198257.

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

H.8 CONTRACTOR RESPONSIBILITY FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

In accordance with the Office of Management and Budget's guidance to Federal agencies and the Nuclear Regulatory Commission's (NRC) implementing policy and procedures, a contractor (including subcontractors and contractor employees), who performs work on behalf of the NRC, is responsible for protecting, from unauthorized access or disclosure, personally identifiable information (PII) that may be provided, developed, maintained, collected, used, or disseminated, whether in paper, electronic, or other format, during performance of this contract.

A contractor who has access to NRC owned or controlled PII, whether provided to the contractor by the NRC or developed, maintained, collected, used, or disseminated by the contractor during the course of contract performance, must comply with the following requirements:

(1) General. In addition to implementing the specific requirements set forth in this clause, the contractor must adhere to all other applicable NRC guidance, policy and requirements for the handling and protection of NRC owned or controlled PII. The contractor is responsible for making sure that it has an adequate understanding of such guidance, policy and requirements.

(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.1 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT. (MAR 2000)

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed May 20, 2022.

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	CSPSS STATEMENT OF WORK
2	CSPSS PRICE SCHEDULE
3	BILLING INSTRUCTIONS FIXED PRICE
4	BILLING INSTRUCTIONS LABOR HOUR
5	NRC 187

Statement of Work (SOW)

1 OBJECTIVE

The Federal Information Security Management Act (FISMA) of 2002 requires agencies to develop, document, and implement an agency wide (includes NRC headquarters facilities, regions, etc.) program for the security of information and information systems that support the operations of the agency. These information systems include those provided or managed by (1) the agency, (2), another agency, (3) Contractor, or (4) other source. Agencies must perform periodic assessments of the risk and magnitude of the harm that could result from the unauthorized use, access, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. The Contractor will assist the NRC in establishing and maintaining a robust Cyber Security Program. The Contractor shall ensure the program operates in compliance with the applicable federal and NRC Cyber Security regulations, policy, standards, and guidance.

The Contractor shall support the NRC as follows:

- Project Management:
  - Maintain a Quality Assurance Plan.
  - Develop and maintain a Project Management Plan.
- Special Projects:
  - Report on cyber security risks across the NRC infrastructure quarterly.
  - Evaluating new technologies to understand their security impact and how they could be used to enhance the NRC Cyber Security Program.
  - Analyze Cyber Security best practices and make recommendations on how those practices could be used at the NRC.
- FISMA Compliance and Oversight:
  - Assist the NRC in authorizing each of its information systems to operate.
  - Support the NRC in establishing and maintaining a robust Cyber Security continuous monitoring program.
  - Assist the NRC with Cyber Security related data calls from other government agencies and the NRC Office of Inspector General.
  - Assess planned or completed remediation actions to ensure they meet federally mandated and NRC defined cyber security requirements.
- Cyber Situational Awareness:
  - Support the NRC's computer security incident response efforts.
  - Perform Computer Security Vulnerability Assessments.
  - Develop and establish and maintain a Cyber Security Laboratory.
  - Verify and validate the agency's use of the Security Content Automation Protocol (SCAP).

- Assist the NRC in establishing a software quality assurance program to verify and validate information systems are resistant to cyber security attacks.
- Perform computer security penetration testing.
- Evaluate system security designs and configurations.
- Develop and implement and maintain an in depth Security Architecture that follows the Federal Segment Architecture Methodology.
- Pilot systems that support the NRC Cyber Security Program.
- Perform Security Impact Assessments (SIAs).

• Policy, Standards, and Training:

- Assist the NRC in developing, establishing, and maintaining Cyber Security Policy that adheres to federally mandated requirements and industry best practices.
- Assist the NRC in developing processes, procedures, templates, checklists, standards, and guidance that support the NRC Cyber Security program.
- Analyze business solutions to ensure they meet federally mandated and NRC defined cyber security requirements.
- Establish, conduct, and maintain IT Security Awareness Training, Role-based Training, and other specialized Cyber Security training.
- Assist the NRC in effectively communicating Cyber Security information to the NRC user community.

2 CONTRACT TYPE

This task order will utilize the firm–fixed-price (FFP) and labor-hour (LH) contract types.

3 SCOPE

The Contractor shall provide all personnel and other direct costs necessary to accomplish the work as specified in this Statement of Work (SOW).

4 FACILITY ACCESS

The following sections provide details on Contractor access to NRC facilities.

4.1 Hours of Operation

The Contractor shall have access to all NRC facilities five (5) days per week, Monday through Friday, except when these facilities are closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. If the Contractor is supporting a critical function (e.g., incident response) their access may be expanded to the weekends. This shall be addressed on a case by case basis.

4.2 Place of Performance

The NRC shall provide onsite physical space for up to four (4) Contractor full time equivalents at NRC headquarters and the NRC shall supply desktops for those individuals to access NRC's Local Area Network (LAN). The remaining Contractor personnel working on this task order shall

operate remotely using a workstation or laptop that has been approved by the primary or alternate COR in writing to process NRC information.

5 TRAVEL

The task order contains the following travel requirements:

(a.) Local travel expenses will not be reimbursed by the NRC. On-site parking at NRC is not available. Parking is available at the White Flint Metro Station.

(b.) Occasional travel to the NRC Regional locations and remote NRC facilities including State and Local Government facilities and external commercial and government application service providers and application hosting facilities may be required.

(c.) Total expenditures for domestic travel (does not include travel to any NRC Headquarters facilities) may not exceed $80,000.00 for each year of the period of performance, without the prior written modification of the task order to obligate additional funds. Travel costs may include an applicable G&A burden but shall not include profit/fee.

(d.) The Contractor will be reimbursed for reasonable travel costs incurred directly and specifically in the performance of this task order. The cost limitations for travel costs are determined in accordance with Federal Acquisition Regulation (FAR) 31.205-46.

(e.) If the Contractor exceeds obligated funds for travel costs, it does so at its own risk.

5.1 Special Access Requirements

The Contractor may need to be contacted outside of normal duty hours. The Contractor shall respond to all inquiries, both during and outside of normal duty hours, within four (4) hours of being contacted by the primary or alternate Contracting Officer's Representative (COR). Historically, this has occurred only a couple of times a year.

6 GOVERNMENT FURNISHED INFORMATION

The Contractor shall have access to information (e.g. Standard Operational Procedures, regulations, manuals, texts, briefs and the other materials associated with this project) and tools located on the NRC infrastructure. All information, regardless of media, provided by the Government and/or generated for the Government in the performance of this task order is Government property and shall be maintained and disposed of by the Government. At the time of disposition, this information shall be boxed up, its contents labeled, and delivered to the Contracting Officer. Also, the Contractor shall completely remove all electronic copies of the information from Contractor equipment (e.g., computers, copiers, printers, faxes). The government reserves the right to verify and validate how this has been done.

All equipment/media that has ever contained electronic copies of SGI or classified information must be provided to the government for destruction.

7 TASKS AND DELIVERABLES

The Contractor shall support the NRC in its efforts to establish and maintain a robust Cyber Security Program. The following tasks shall be performed by the Contractor during the execution of this Statement of Work. All data that is first produced under this task order is subject to clause 52.227-17, Rights in Data—Special Works (Dec 2007).

All deliverables must be provided to the primary COR and their alternate COR (s) in the NRC Computer Security Office (CSO).

The primary and alternate COR (s), in consultation with the NRC CISO, will provide overarching technical direction on the manner and method used to perform and report on all cyber security activities and shall resolve any differences in technical direction provided by different office CORs.

Note: This task order cannot be awarded to a Contractor that constructs, operates, or maintains NRC information systems. This would be considered a conflict of interest. Also the Contractor will not be allowed to act as an Information System Security Officer (ISSO) for any NRC system.

7.1 Project Management

The Contractor shall comply with, and provide the following services as required by, NRC Management Directive 2.8, Project Management Methodology (PMM).

7.1.1 Quality Assurance Plan

The Contractor shall provide a Quality Assurance Plan for this task order. This plan must be approved in writing by the primary or alternate COR (s) prior to submission of the first deliverable. The plan shall address the following:

1) Deficiency Prevention: A description of the methods to be used for identifying and preventing deficiencies and their causes in the quality of service performed before the level of performance becomes unacceptable.

2) Resolution: Documents the corrective or preventive actions that were taken during the execution of this task order. These records shall be made readily available to the primary and alternate CORs.

7.1.2 Project Plan (includes Level 4 Work Breakdown Structure)

The Contractor shall develop and maintain a Project Plan for this task order and provide that project plan electronically to the primary and alternate CORs. At a minimum, the project plan shall contain a Level 4 Work Breakdown Structure (WBS) and shall use the project plan template from NRC's PMM web site. 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 have a short duration (not to exceed 80 hours), or can be divided into a series of milestones whose status can be objectively measured. Each work package shall be assigned a start and finish date, a budget value, and shall be constructed such that it can be integrated with higher-level schedules.

Levels one through three of the WBS shall be organized as follows:

- **Level one** of the WBS shall represent the NRC Office that is allocating funds on this task order. The Contractor must be able to track costs and earned value management at this level.
- **Level two** of the WBS shall be broken down into various activities that are being performed for that NRC Office. For example: Continuous Monitoring, Authorization, Software Quality Assurance, Policy Support, Standards Support, etc.

- **Level three** of the WBS shall represent the tasks that are needed to perform each activity under this task order. For example under Authorization: Security Categorization, System Security Plan, Standards Test & Evaluation Plan, Testing, etc.

The project plan shall specify, at the task level, a schedule and ceiling price to accomplish the work and identify the resources needed to complete the work. Resources include manpower, hardware, software, equipment, travel, etc. The Contractor shall ensure the WBS laid out in the project plan adequately defines all work necessary to meet the requirements of this task order.

The Contractor shall utilize Microsoft Project and other resources to develop and maintain the project plan. The project plan shall be provided to the primary and alternate CORs on a monthly basis and shall be delivered in conjunction with the Monthly Status Report.

7.2 Special Projects

The following Special Projects shall be implemented under this task order.

7.2.1 Assessment of Residual Risk

The Contractor shall develop and implement a process for determining cyber security risks that affect the NRC IT infrastructure. The Contractor shall place greater emphasis on risks that occur at an enterprise level or impact multiple NRC information systems. The Contractor shall develop a reporting template (Quarterly Residual Risk Report) and brief the primary and alternate CORs on current residual risks as well as risk trends on a quarterly basis.

Assessment of risks shall be based upon supported evidence. The Contractor shall use the following sources to determine these risks: audits, the Enterprise Risk Assessment, Cyber Security incidents, NRC Strategic Plans, Inspector General Reports, Plan of Action & Milestone items, vendor reported vulnerabilities & exploits, and observations. The Contractor shall identify, prioritize, and map these risks to NRC's mission and business functions. The Contractor shall document all risks that were found during this assessment in a formalized report that is delivered to the primary and alternate CORs.

The Contractor shall give a quarterly risk briefing to the primary and alternate CORs that communicates the results of this assessment to NRC management.

7.2.2 Classified Processing Support

The Contractor shall provide the following security engineering support for classified information processing:

- Support the NRC efforts to obtain an authorization to operate for systems that process classified information.
- Assist the NRC in developing and maintaining a continuous monitoring program for its information systems that process classified information.
- Work with the NRC to ensure that classified information is properly protected and secured.

All classified processing must comply with CNSS publications, except where the information and systems are governed by the Director of National Intelligence issuances.

7.2.3 Evaluation of New Technologies

The Contractor may be requested to assist the primary and alternate CORs in evaluating new technologies so the impact these technologies have on NRC's information systems and the NRC Cyber Security Program can be fully understood.

7.2.4 Analysis of Best Practices

The Contractor shall analyze security best practices to determine how those practices can be applied to the NRC Cyber Security Program. After the analysis has been completed, the Contractor shall develop recommendations and document those recommendations in white papers that will be delivered to the primary and alternate CORs. Once the primary or alternate COR has reviewed the white papers and decided upon a course of action, the Contractor m primary and alternate CORs may be asked to assist the NRC in incorporating selected recommendations into the NRC Cyber Security Program.

7.3 System Authorization

The Contractor shall assist the NRC with the following: authorizing its information systems, developing accurate and high-quality system security documentation, testing systems to determine risk, supporting continuous monitoring activities, and assisting with data calls from other government agencies and the NRC Office of Inspector General (OIG).

7.3.1 Obtaining NRC Information Systems Authorization to Operate

The Contractor shall assist the NRC in developing authorization packages for its unclassified information systems. The Contractor may support the system owner in the development of the entire authorization package or just a portion of it. For example, the Contractor may only act as an independent assessor during the testing and evaluation of the system. In this instance the Contractor would only be testing the system.

The Contractor shall assist the NRC in annually authorizing NRC information systems. An authorization package must include but is not limited to the following:

- E-Authentication Risk Assessment

  Electronic authentication (e-authentication) is the process of establishing confidence in user identities electronically presented to an information system. The focus is on remote authentication of individual people over a network, for the purpose of electronic government or commerce. The OMB M-04-04 memorandum guidance applies to systems that have remote authentication of users of Federal agency information technology systems for the purposes of conducting Government business electronically (or e-government). The guidance does not apply to internal only systems or the authentication of servers, or other machines and network devices. E-Authentication Risk Assessments shall be consistent with OMB M04-04, NIST SP 800-30, NIST SP 800-60, and NIST SP 800-63. The Contractor must develop the E-Authentication Risk Assessments according to NRC requirements. It will be the responsibility of the Contractor at the start of each assessment to ensure the latest requirements are adhered to.

- Security Categorization Package

  Security categorization for information and information systems provides a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs; (ii)

consistent reporting to the OMB and Congress on the adequacy and effectiveness of cyber security policies, procedures, and practices. NRC's Security Categorization Package contains the following deliverables: Security Categorization Memo, Security Categorization Document, Privacy Impact Assessment (PIA), etc. The Security Categorization document must follow federally mandated requirements found in NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems and NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories. In addition, the Contractor must develop the Security Categorization Package according to NRC defined cyber security requirements. It will be the responsibility of the Contractor at the start of each categorization package to ensure the latest requirements are adhered to.

- Security Risk Assessment (SRA)

  The SRA is an important activity in the NRC's information security program that directly supports security authorization and is required by the FISMA and OMB Circular A-130, Appendix III. This assessment influences the development of the security controls for an information system and generates much of the information needed for the system's security plan.

  The assessment shall ensure compliance with NRC's Cyber Security policy, ensure compliance with federally mandated security requirements, and include but is not limited to the following:

  - Identification of user types and associated roles and responsibilities;
  - Identification of risk assessment team members and their associations;
  - A description of the risk assessment approach and techniques, where the techniques include documentation review, interviews, observation, and system configuration assessments, security scans and penetration tests;
  - A description of the risk scale used, including at a minimum, the potential impact as defined in FIPS 199, and likelihood as defined in NIST SP 800-30, Risk Management Guide for Information Technology Systems;
  - A list of potential system vulnerabilities;
  - A list of potential threat-sources applicable to the system, including natural, human, and environmental threat-sources;
  - A table of vulnerability and threat-source pairs and observations about each;
  - Detailed findings for each vulnerability and threat-actions discussing the possible outcome if the vulnerability was exploited; existing controls to mitigate the pair; the likelihood determination as high, moderate, or low; the impact determination expressed as high, moderate, or low; the overall risk rating based upon the risk scale; and the recommended controls to mitigate the risk; and,
  - A summary that includes the number of high, moderate, and low findings and provides a list of prioritized action items based upon the findings.

  The assessment shall be documented in a report according federally mandated and NRC defined cyber security requirements. It will be the responsibility of the Contractor at the start of each assessment to ensure the latest requirements are adhered to.

All findings that are discovered during the SRA shall be incorporated into the system's Plan of Action and Milestones (POA&M) Report.

- System Security Plan (SSP)

  The SSP shall be developed in accordance with NRC Cyber Security policy and federally mandated requirements (NIST Special Publications, Federal Information Processing Standards, etc.). The SSP identifies the necessary security controls that are required, citing the security controls that are in place, those that are planned, those that are not planned, and those that are not applicable.

  When an NRC information system inherits a security control being provided by another information system, what is being inherited shall be noted along with the name of the system providing that control. The Contractor shall trace the security controls to specific documented guidance, NRC policy (e.g., Management Directives), infrastructure policy or procedures, and federally mandated security requirements.

  The SSP shall be documented and updated to reflect security testing, control implementation, and changes to the system. Once the certifier enters his/her information into the SSP it cannot be changed without CSO's approval. The final SSP shall reflect validated in-place and planned controls.

- Preliminary Assessment Report

  The Contractor shall perform a preliminary assessment of the system to ensure the system is compliant with federally mandated and NRC defined cyber security requirements. The following is a sample of what must be checked:

  - All National Institute of Standards and Technology (NIST) Federal Information Processing Standards. Especially NIST FIPS 140-2. When checking NIST FIPS 140-2, the Contractor must ensure that all cryptography used in the system has been validated, has a current FIPS 140-2 certificate, and the configuration of that cryptography complies with the security policy specified by the certificate for the cryptographic module.
  - All NIST Special Publications. Especially NIST 800-53. The Contractor must ensure the system complies with the technical, managerial, and procedural controls found in this standard.
  - All NRC Management Directives.
  - All NRC Cyber Security Standards. For a complete list of Cyber Security standards please see "http://www.internal.nrc.gov/CSO/standards.html".

    Note: If a configuration standard has not been identified, DISA standards, checklists, and guidance shall be used. In the absence of CSO and DISA configuration information, CIS benchmarks shall be used. In the absence of CSO, DISA, and CIS configuration the vendor's security guide shall be used.
  - Currency of Cyber Security relevant patches, service packs, and versions.
  - Mitigation of known vulnerabilities
  - All Committee on National Security Systems (CNSS) issuances

  The Contractor shall identify any operational risks found that may affect the system's ability to perform its mission and protect its data (stored and transmitted). The Contractor shall

assist developers, project managers, engineers, etc. to identify vulnerabilities during the initial stages of the System Development Life Cycle (SDLC).

Preliminary Testing includes automated and manual testing of the different system platforms to ensure they have been configured, operated, and maintained correctly and in accordance with NRC policy and standards. An operating system and application scan against required configuration standards and assessing vulnerability patching is required.

The Contractor shall document the results and observations of this process in a Vulnerability Assessment Report (VAR). Each finding identified in the VAR shall include the risk number, a description of each risk, the type of risk (i.e., impacting the confidentiality, integrity, or availability), the level of risk (i.e., low, moderate, or high), the associated controls, and the action(s) required or actually performed to eliminate or minimize each risk.

The Contractor shall coordinate and execute all applicable site access and non-disclosure agreements and authority to scan forms with parties other than the NRC prior to commencement of the above mentioned activities, ensuring that project schedules are not impacted.

Finally, all deficiencies found in the system that are exploitable must be reported to the primary and alternate CORs immediately in writing.

- Systems Test and Evaluation (ST&E) Plan

  The ST&E plan exercises the system's security controls and ensures those controls are operating as intended and have been implemented in accordance with federally mandated requirements / NRC defined surety requirements. The following lists some of the guidance that should be considered when developing the ST&E Plan:

  - NIST SP 800-53A Guide for Accessing the Security Controls in Federal Information Systems
  - NIST SP 800-53 Recommended Security Controls for Federal Information Systems
  - NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems
  - NRC System Security Test and Evaluation Plan Template

  The ST&E plan provides detailed test procedures to ensure all federally mandated and NRC defined cyber security requirements are fully tested. These procedures contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures.

  The following criteria shall be utilized during testing:

  - **Examine -** The Contractor shall observe random individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. For example, examine visitors upon computer room entry in order to verify that all visitation procedures are followed. The Contractor shall examine all processes, procedures, and documents associated with the system to ensure they are in compliance with established requirements.

- **Interview -** The Contractor shall interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.
- **Inspection -** The Contractor shall ensure security controls have been properly implemented and maintained. For example, the Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.
- **Test -** The Technical Test verification method shall be used to verify that each implemented control is functioning as intended. For example, the Contractor shall attempt to access the system by logging on to the system from an end user workstation (or other device) using an incorrect password to see if the system responds with an error message stating an incorrect password has been entered or denies access after exceeding the maximum threshold for logon attempts.

If a control is inherited, the Contractor shall review the inherited system's security documentation to determine if the control is in place and operating as intended. If it is not, this shall be factored in when the system's risks are determined.

If the control is not inherited, the Contractor shall ensure that the security control meets all federally mandated and NRC defined cyber security requirements and provides the appropriate level of protection based on the sensitivity of the system. This shall be determined through interviews, documentation reviews, or testing.

- Security Control Testing

The system shall be reviewed, verified, and validated using the system's security test plans and procedures to ensure the accuracy and adequacy of documented test procedures for all system security controls 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 evaluate common controls used throughout the agency. Once testing has been completed, the ST&E Report, the Vulnerability Assessment Report, and the Project Objectives and Milestones (POA&M) Report shall be developed to document the results. All findings that are not immediately remediated must be documented.

System testing includes automated and manual testing of the different system platforms and applications to ensure security controls have been configured, operated, and maintained correctly. This shall be accomplished through interviews, documentation reviews, or testing depending on the security control being assessed.

The Contractor shall be responsible for coordinating and executing all applicable site access, and authority to scan forms with other parties for the commencement of the above mentioned activities.

Examples of some of the standards that must be checked:

- National Institute of Standards and Technology (NIST) Federal Information Processing (FIPS) 140-2. When checking NIST FIPS 140-2, the Contractor must ensure that all cryptography used in the system has been validated, has a current FIPS 140-2

certificate, and the configuration of that cryptography complies with the security policy specified by the certificate for the cryptographic module.

- NIST 800-53A. The Contractor must ensure the system complies with the technical, managerial, and procedural controls found in this standard.
- NRC Cyber Security Standards. NRC Cyber Security standards ensure a consistent application of security across NRC information systems and provide a minimally acceptable level of security for devices, operating systems and applications. NRC Cyber Security Standards are used as system baseline configurations for any information system that stores, transmits/receives, or processes NRC information.

Please note: Individual Contractors working with the system owner to develop the system's E-Authentication Risk Assessment, Security Categorization Package, or SSP cannot be involved in system testing. This would be considered a conflict of interest.

- POA&M Report

  The POA&M Report identifies the risks or findings that were found during the authorization process. POA&Ms document the risk number; a description of each risk; the type of risk (i.e., impacting the confidentiality, integrity, or availability); the level of risk (i.e., low, moderate, or high); the associated controls; and the action(s) required or actually performed to eliminate or minimize each risk. The POA&M report is a tool that is used to track the system's remaining findings to ensure remediation occurs over an agreed upon period of time.

  The format and data required in quarterly POA&M reports is determined by the OMB and is subject to change on an annual basis.

- Contingency Plan (CP)

  The Contractor shall assist the NRC in developing a CP, disaster recovery procedures, and business impact assessment that supports the system's contingency planning process. The CP shall be documented according to the current NRC CP Template.

  The CP shall be developed in accordance with federally mandated requirements, NRC defined cyber security requirements and contingency approach, National Institute of Standards & Technology (NIST) Special Publication (SP) 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems", and the NRC Contingency Plan (CP) Template.

  The Contractor shall document detailed procedures for the Notification/Activation Phase, Recovery Operations, and Return to Normal Operations. The procedures shall contain sufficient detail that a technically trained individual not familiar with the system can successfully follow the procedures. The system CP shall contain but will not be limited to the following:

  - Sufficient contact information (personnel and vendor)
  - Equipment (hardware and software)
  - Specification information to enable reconstitution of the system from scratch, all service level agreements, memoranda of understanding

- IT standard operating procedures for the system
- Identification of any systems that this system is dependent upon along with references for the applicable contingency plans
- References to the emergency management plan and occupant evacuation plan
- References to the appropriate continuity of operations plan.

- Contingency Plan Test Report

  The Contractor shall provide expert advice and support during the Contingency Plan Test to ensure the test is documented in accordance with the system's CP, federally mandated requirements (NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems", etc.), and NRC defined cyber security requirements.

  The test shall be documented using a template approved by the primary or alternate CORs. The Contractor shall update the system's CP once the CP Test Report has been completed to reflect validated information. The primary or alternate CORs must approve the final version of the system's CP and Contingency Plan Test Report.

- Authorization Package

  The Authorization package provides the authorizing official with the essential information needed to make a credible risk-based decision on whether to authorize operation of the information system. The Authorization Package contains the following deliverables: Security Categorization Document, SRA, SSP, ST&E Plan, ST&E Report, Vulnerability Assessment Report, POA&M Report, and an Approval to Operate Request Memo.

  The ST&E Execution Report, VAR, and Contingency Plan Test Report shall be delivered in a file format that cannot be changed.

  The SSP, SRA, ST&E Plan, ST&E Report, and VAR must be current (within 2 months).

  If the system has a risk that cannot be mitigated or captured on the POA&M report, the risk must be captured in a Deviation Request. Some findings cannot be remediated because they will break the system or impact its business objectives. For these findings a deviation request is developed that justifies why this finding has not been addressed, what is the risk to the system and NRC infrastructure, and what are the mitigating controls in place that protect the system from this risk.

- Supporting Documentation

  The Contractor shall develop documentation that supports the system's authorization package (standard operating procedures, service level agreements, memorandums of understanding, interconnection agreements, etc.). The Contractor shall ensure all supporting documentation has been identified, properly developed, and has addressed all federally mandated and NRC defined cyber security requirements.

7.3.2 Obtaining Laptop Authorization to Operate

The contactor shall conduct Laptop System Authorizations for NRC system owners.

Laptops must comply with all federally mandated and NRC defined cyber security requirements. Once properly configured, the system owner (NRC office director or Office of Information Systems division director) certifies the laptop system and sends a memo to the CISO notifying them that the laptop system is ready to be evaluated. CSO reviews the system owner's submittal, all supporting documentation, and provides a recommendation to the DAA if the laptop should be authorized.

7.4 Continuous Monitoring Support

The Contractor shall assist the primary and alternate CORs in establishing and maintaining a continuous monitoring process that addresses federally mandated and NRC defined cyber security requirements. Currently, the NRC performs Continuous Monitoring activities on 30 systems.

The continuous monitoring process shall consist of but is not limited to the following:

- Coordinate Continuous Monitoring Efforts
  - Coordinate the continuous monitoring efforts.
  - Assist the system owner's representatives in establishing their continuous monitoring schedules.
  - Apply knowledge, skills, tools, and techniques to ensure continuous monitoring activities are performed effectively, on schedule, and within budget.

- Perform Annual Security Controls Testing

  The Contractor shall conduct annual security controls testing of the organization's information systems according to NIST SP 800-53 "Guide for Assessing the Security Controls in Federal Information Systems" and NRC Cyber Security requirements. The Contractor shall work with the NRC to develop selection criteria to determine which security controls shall be tested to include common controls and inherited controls. At a minimum, the selection criteria shall be based upon: the sensitivity level of the system; the requirement to annually test volatile controls; controls called out for annual testing in OMB guidance; CSO specified controls; and those associated with each system's POA&M items. This assessment shall be performed on all NRC Information Systems each fiscal year.

  The Contractor shall perform a comprehensive assessment of the selected programmatic, management, operational, and technical security controls for each system. The assessment shall determine the extent to which each system's controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting federally mandated and NRC defined cyber security requirements. Upon completion of testing, the Contractor shall develop an Annual Security Controls Test Report for each system and incorporate any findings into that system's POA&M Report.

  The draft Annual Security Controls Test Report and the updates made to the system's POA&M Report shall be submitted to NRC review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions.

- Conduct Quarterly Scanning

  The Contractor shall conduct quarterly vulnerability scanning of NRC's systems. Quarterly scanning shall establish if the system's security controls are operating as intended and

ensure systems continually meet federally mandated and NRC defined cyber security requirements. All risks / deficiencies shall be measured according to NIST SP 800-30 "Risk Management Guide for Information Technology Systems".

The Contractor shall use a variety of testing tools (Nessus, Core Impact, DISA Gold, Air Magnet, etc.), manual and automatic, including proprietary and modified open source, to conduct the assessment. All hardware and software used to support this task order must be approved in writing by the primary or alternate CORs.

Scanning shall consist of the following phases:

- **Phase 1: Preparation –** The Contractor shall ensure all testing devices that are going to be used during the assessment are loaded with the latest patches, security updates, device drivers, and plug-ins.
- **Phase 2: Information Gathering –** The Contractor shall conduct scans, review documentation, and interview personnel to gather the needed information to perform a risk analysis of the organization's systems.
- **Phase 3: Draft Assessment Reports -** The Contractor shall develop System Assessment Reports that identify the risks each system poses to itself, its data, and the NRC infrastructure.
- **Phase 4: Validate Findings –** The Contractor shall validate findings, ensure risks have been properly assessed, and develop mitigation strategies that will address deficiencies in consultation with the System Owner, ISSOs and System Administrators.
- **Phase 5: Finalize Assessment Reports –** The Contractor shall incorporate NRC's comments into the Assessment Reports and deliver the final version of the Assessment Reports to the primary and alternate CORs.
- **Phase 6: Plan of Action and Milestone (POA&M) Reports –** The Contractor shall incorporate any findings into each system's POA&M Report.

The Contractor shall submit Assessment Reports and Updated POA&M Reports to the primary and alternate CORs for review and comment. The Contractor shall revise and update each deliverable as appropriate based on written feedback from the primary and alternate CORs and provide final versions to the primary and alternate CORs.

- Update POA&M Reports

The Contractor shall update system level POA&M reports quarterly. When updating POA&M reports, the Contractor shall utilize the CSO POA&M Quality Checklist and review the report with the CSO to ensure the report is in accordance with the CSO POA&M process.

The Contractor shall collect information so the POA&Ms can be updated to reflect the current situation. Any new vulnerability that is discovered shall be added and assigned to the appropriate system. All POA&M Reports shall be submitted for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the primary and alternate CORs.

Upon completion, the Contractor shall upload the POA&M Reports into the CSO FISMA Compliance automated tracking tool.

- Update Contingency Plan

  The Contractor shall update the system level CPs and ensure the CP is still valid and effective. The System CP shall be documented in a report that follows the NRC Template. The CP shall be maintained in its hard copy form for contingency execution should the NRC Network Infrastructure be unavailable.

- Develop Contingency Plan Test Reports

  The Contractor shall ensure the Contingency Planning Test is documented in accordance with the system's CP, federally mandated requirements (NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems", NIST SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems", etc.), and NRC defined cyber security requirements.

- Update SRA and SSP

  Annually, the Contractor shall update the system's SRA and SSP. The draft documents shall be submitted to the organization for review and comment. The Contractor shall revise and update each deliverable as appropriate and provide final versions to the primary and alternate CORs.

  This activity should be performed in conjunction with the Annual Security Controls Testing.

- Provide Security Engineering Support

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

  The Contractor shall keep all supporting documentation up-to-date (memoranda, agreements, procedures, etc.) in consultation with the CSO.

7.5 Data Calls

The Contractor shall assist the NRC's in its efforts to respond to Cyber Security related data calls from the NRC OIG and other government organizations. Data calls are usually unexpected and require a quick turnaround.

7.6 Cyber Situational Awareness

The Contractor shall provide the following services.

7.6.1 Incident Response Efforts

The Contractor shall assist the NRC in developing, establishing, and maintaining an agency wide Incident Response Program that addresses federally mandated and NRC defined cyber security requirements (found in Management Directives and policy).

At a minimum the Incident Response Program shall satisfy the following criteria:

- **Incident Response Process And Procedures** - Develop, disseminate, and review/update formal incident response procedures that address purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance with federally mandated and NRC defined cyber security requirements.

- **Incident Response Training** - Train personnel in their incident response roles and responsibilities with respect to the information system; and provide refresher training annually. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations. Employ automated mechanisms to provide a more thorough and realistic training environment. Ensure closed incidents are reviewed for lessons learned. Lessons learned should be incorporated into Incident Response processes, procedures, and plans.
- **Incident Response Testing And Exercises** - Test the incident response capability for the information system annually using defined tests and/or exercises to determine the incident response effectiveness and document the results. Employ automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.
- **Incident Handling** – Implement an incident handling capability that includes:
  - Preparation for security incidents.
  - Verification and validation of the organization's detection, declaration, containment, remediation, and restoral capabilities.
  - Coordination of incident handling activities and contingency planning activities.
  - Incorporation of lessons learned from historical incident handling activities to enable continuous improvement of the agency's incident handling program.
  - Deployment of automated mechanisms to support the incident handling process.
  - Identify classes of incidents (e.g., targeted malicious attacks, untargeted malicious attacks, malfunctions due to design or implementation errors and omissions) and define appropriate actions to ensure continuation of mission/business operations.
  - Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
  - Implement a configurable capability to automatically disable an information system if a set organization defined security violations are detected.
- **Incident Monitoring** - Track and document information system security incidents. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
- **Incident Reporting**. Employ automated mechanisms to assist in the reporting of security incidents. Report information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
- **Incident Response Assistance** - Provide an incident response support resource that offers advice and assistance to users of NRC information systems for the handling and reporting of security incidents. .
- **Incident Response Plan** - Develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability; describe the structure of the incident response capability; provide a high-level approach for how the incident response capability fits into the overall organization; meet the unique requirements of the NRC, which relate to mission, size, structure, and functions; define reportable incidents; provide metrics for measuring the incident response capability within the NRC;

and define the resources and management support needed to effectively maintain a mature incident response capability. Distribute copies of the incident response plan to specified personnel. Review the incident response plan annually. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. Communicate any changes to the incident response plan to specified personnel.

7.6.2 NRC Enterprise Security Architecture

The NRC Enterprise Security Architecture (ESA) is envisioned to be an integral and critical component within the overall NRC Enterprise Architecture.

Recent studies, by both the Government Accountability Office (GAO) and the Computer Security Institute found that the number of cyber security threats to both the government and the private sector continues to be on the rise. The potential for damage to both the physical critical infrastructure and the ability for the United States to effect continuity of government could be greatly impacted or denied by successful attacks. The NRC is not exempt from this continuing and persistent threat. The Contractor shall assist the NRC in building and sustaining the agency ESA.

The NRC has acknowledged that cyber warfare applies to all systems. As a result, the Computer Security Office seeks to provide and build, a sustainable Enterprise Security Architecture, wherein the following principles drive the task deliverables:

- Security levels applied to resources should be commensurate to their value to the organization and sufficient to contain risk to an acceptable level.
- The architecture must accommodate varying security needs.
- The architecture must provide integrated security services to enable the enterprise to conduct safe and secure business electronically.
- A single, accurate and consistent system date and time should be maintained across the enterprise architecture and security elements to enable service-wide root cause analysis, response and containment. Users will see the time local to their geographic location.

The objectives within the NRC ESA Program include, but are not limited to:

- Ensuring that the NRC IT Infrastructure, IT Services, system software and components as articulated in the ESA continually enable the appropriate risk based protection of NRC information and information systems.
- The target ESA, along with other NRC Computer Security Office solutions and deliverables will at a minimum, support the 2010 Federal Information Security Management Act Reporting Requirements for all executive agencies.
- The target ESA will support HSPD-12, IPv6, as well as the latest published, released version of the Federal CIO Council Information Security Line of Business and Security and Privacy Profile.
- The target ESA will support the cyber security requirements established by Federal and NRC regulations, statues, standards and guidance pertaining to NRC information

confidentiality, accessibility, availability and integrity.

- The "as-is" and target Enterprise Security Architectures shall enable rapid visibility into the current security posture of the NRC IT operational environment and provide insight into the desired security posture.

- The ESA shall enable the NRC to assess the maturity of the operational environment using the latest version of the SANS Institute Consensus Audit Guidelines.

- The ESA shall support the secure, efficient transaction of business and delivery of services. The ESA shall support the Separation of Duties Principle.

- The Contractor shall develop and maintain the NRC Enterprise Security Architecture (ESA) Principles and Framework to provide a continuing risk-based, defense-in-depth security architecture to protect the confidentiality, integrity and availability of the agency's sensitive information and information network(s) and systems.

- The Contractor shall ensure that the ESA is a subset of and maintains alignment with the NRC and the Federal Enterprise Architecture models.

- The Contractor shall develop and maintain the "as-is" architecture, the target or "to-be" architecture and the agency transition strategy to migrate from one to the other. The target architecture should project no more than 3 years into the future as technology continues an ever-tighter evolutionary cycle.

- The ESA shall be developed in conjunction with the NRC Strategic Plan, the NRC IT / IM Roadmap and the current release of the NRC Technical Reference Model and IT Services Catalog.

- The Contractor shall use the current, published release of the Federal Enterprise Architecture and the Federal Segment Architecture Methodology in development of the NRC ESA.

The primary and alternate CORs will evaluate and measure Contractor progress and ESA capability maturity using, at a minimum, but not limited to, the most current, published release of the Government Accountability Office Document entitled "*Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management*". The most current release is Version 2.0. The Contractor is encouraged to incorporate this framework and their assessment for each of the deliverables as appropriate.

Additionally, the Contractor shall meet with the primary and alternate CORs once per month to discuss status and challenges associated with this effort. The Contractor shall provide the following deliverables to the NRC in support of this work as follows:

ESA Deliverable 1 – The Annual Enterprise Security Architecture (ESA) Project Plan - This plan shall describe the scope (requirements), time, cost, resources and risks associated with the development, sustainment and maturity of the ESA and all subsequent ESA task order deliverables. The Contractor shall use the NRC Management Directive 2.8 Project Management Methodology (PMM) to construct the Integrated Master Schedule. The NRC PMM leverages the IBM Rational Unified Process (RUP) four key life-cycle phases, inception, elaboration, construction and transition. The Integrated Master Schedule must provide sufficient

definition to track each sub-task against time, scope, resources, risks and quality. Each version of the annual plan will be reviewed and approved by the primary and alternate CORs, will be based-lined, and the Contractor shall provide updates to the primary and alternate CORs no less than once per quarter.

ESA Deliverable 2 - The Enterprise Security Architecture (ESA) Charter and Communications Plan - The Contractor shall develop and update, with inputs from the primary and alternate CORs, those core NRC organizations that have a measurable requirement in the development, responsibility and communication of the Enterprise Security Architecture across the agency to facilitate its acceptance and institutionalization within each applicable NRC Office. .

ESA Deliverable 3 - The Annual "as-is" Enterprise Security Architecture - The ESA shall use the Federal Segment Architecture Model to capture, articulate and report, at a minimum, but not limited to, the existing policies, security standards, standard operating procedures, services and components that form the agency's current cyber security infrastructure. The "as-is" ESA should be validated by the Contractor against the currently operational environment and the latest version of the NRC Technical Reference Model through manual and automated means available.

ESA Deliverable 4 - The Annual Target Enterprise Security Architecture - Using the NRC Strategic Plan, the NRC IT Roadmap, the NRC Technical Reference Model, the CSO Residual Risk Reports, the NRC implementation maturity of the SANS Consensus Audit Guidelines as well as authoritative reports and information provided by NRC Offices, the NRC Office of the Inspector General, the Governmental Accounting Office, the Department of Homeland Security, the Department of Justice, the National Institute of Standards and Technology, the NRC Trusted Internet Connection (once operational), and the principles contained in this task and the ESA Charter, the Contractor shall use the Federal Segment Architecture Methodology to develop the Annual Target Enterprise Security Architecture.

Each deliverable shall include a draft for comment and the Contractor shall meet with the primary and alternate CORs to discuss items that need improvement.

7.6.3 Vulnerability Assessments

The Contractor shall conduct vulnerability assessments. A vulnerability assessment is an independent verification and validation of a system's security controls, cyber security requirements, technical resolutions, risk mitigations, and implementations that identifies the deficiencies and vulnerabilities that are present in the system. This helps the NRC determine levels of risk present in the system and if those risks are acceptable.

The testing methodology, assumptions, constraints, and dependencies must be clearly stated up front so the results can be put into proper context. Also, the personnel, hardware, and tools used to perform the test must be identified.

The Contractor shall ensure testing identifies any operational risks found that may affect the system's ability to perform its mission, protect its data (stored and transmitted), or make the NRC infrastructure vulnerable.

The following test methods shall be used:

- **Analysis** - The "analysis" verification method shall be used to appraise a process, procedure, or document to ensure properly documented actions (e.g. risk assessments,

audit logs, organization level policies, etc.) are in compliance with established requirements. An example of "analysis" as an evaluation technique would be to review documented physical security policies and procedures to ensure compliance with established requirements. This verification method is often called a documentation review.

- **Demonstration -** The Contractor shall observe random individuals to verify that activities on the system follow the documented procedure or process as the activity is performed. For example, observe visitors upon computer room entry in order to verify that all visitation procedures are followed.
- **Interview -** The Contractor shall interview personnel to verify the security policies and procedures are understood as implemented and prescribed by governing policies and regulations.
- **Inspection -** The Contractor shall ensure security controls have been properly implemented and maintained. For example, the Contractor shall verify that the visitor's name, signature, organization, reason of visit, arrival and departure date, time, and the escort's name, initials, or signature are included on the log sheets.
- **Technical Test -** The Technical Test verification method shall be used to verify that each implemented control is functioning as intended. For example, the Contractor shall attempt to access the system by logging on to the system from an end user workstation (or other device) using an incorrect password to see if the system responds with an error message stating an incorrect password has been entered or denies access after exceeding the maximum threshold for logon attempts.

Testing shall be accomplished using interviews, documentation reviews, or scanning depending on the security control being assessed.

7.6.4 Source Code Reviews

The Contractor shall implement a program that gives the NRC the capability to scan object files for vulnerabilities and deficiencies. Under this program two capabilities will be established:

- Developer Verification – The Contractor will evaluate auditing software used by NRC's IT system developers so flaws and inadequacies that exist in their source code can be identified, prioritized, and understood.
- CSO Verification – NRC uses offsite software as service (SAAS) to provide code validation to ensure developed source code has been properly hardened and is resistant to known attacks.

By utilizing these capabilities, the NRC will be able to develop a robust program that ensures customized source code is properly protected from attackers.

7.6.5 Penetration Testing

The Contractor shall conduct external and internal ("red team" and "blue team") penetration tests and social engineering tests against the NRC infrastructure and its user community. The Contractor shall use a variety of testing tools, manual and automatic, including proprietary and modified open source, to attempt to penetrate NRC systems. The primary or alternate CORs must be present during all active penetration testing.

The following steps shall be followed:

- **Phase 1: Information Gathering** – The Contractor shall gather information and perform an analysis identifying the touch points that need to be tested (for example: publically facing servers, routers, firewalls, gateways, remote access services, web applications, adherence to policies & standards, etc.).
- **Phase 2: Testing Tools** – The Contractor shall develop a Tools Report that identifies the automated tools that are going to be used for testing. The tools report must be approved by the primary or alternate CORs in writing before the Contractor can move on to the next phase.

  The Contractor shall update all devices that are going to be used during the tests with the latest patches, security updates, device drivers, and plug-ins. The devices used during the tests will be wiped once the tests have been completed.

- **Phase 3: Test Plan** - The Contractor shall develop a detailed Test Plan that describes the penetration testing, and social engineering attacks that are going to be performed against the NRC. The Test Plan must be approved in writing by the primary or alternate CORs before any testing can be initiated. The Test Plan will answer the following questions:
  - Who will be performing the test?
  - What tools are going to be used?
  - What tests are going to be run against the NRC's automated information systems and user community?
  - When are the tests going to be run (date and time)?
  - Where will the tests be conducted from?
  - How are NRC automated information systems and users going to be affected?
  - How is Contractor going to identify the risk?
- **Phase 4: Testing** - The Contractor shall perform external penetration testing, internal penetration testing, and social engineering attacks against the NRC under observation by a designated government official. All raw scans, observations, and testing results shall be captured and documented in the corrective action report.
- **Phase 5: Test Result Report** – The Test Result Report shall contain but will not be limited to the following:
  - Summarize how each test was performed and how the risk was evaluated.
  - Identify each type of test that was run (external penetration test, internal penetration test, and social engineering attack).
  - Specify the hosts/users that were tested and the information systems/organizations they belonged to
  - 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 6: Cleanup** – The Contractor shall wipe all devices used during testing and certify in writing that the task was completed. All Contractors associated with this task order 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.

All testing must be approved in writing by the primary or alternate CORs. The Contractor will not conduct any testing without written approval from the primary or alternate CORs and without being under the primary or alternate COR's observation.

7.6.6 Security Impact Assessments

The Security Impact Assessment (SIA) process helps determine the necessary steps a system owner must take to incorporate a change into an NRC approved information system. The system owner must summarize the change by filling the SIA form, send that form to the CSO for review, and finally the CSO informs the system owner on what must be done to ensure the change does not negatively impact the security posture of the information system or NRC infrastructure.

The Contractor will assist NRC system owners in gathering information, filling out the SIA form, and interpreting guidance from the primary or alternate CORs on what needs to be done. Representative types of activities that may be required include:

- Updating Security Categorization Packages
- Updating Authorization documents
- Conducting a tailored ST&E that includes only the changes that are made to the system
- Developing a vulnerability assessment report that describes the technical risks associated with the change
- Assessing how the change impacts other NRC information systems or the NRC infrastructure

7.7 Policy, Standards, and Training

The Contractor shall provide the following services.

7.7.1 Cyber Security Policy

The Contractor shall support the NRC efforts to ensure that all aspects of Management Directive and Handbook (MD) 12.5 properly address Federally mandated requirements, (through gap analyses, vulnerability assessments, etc.), properly communicated to the NRC user community, and kept up-to-date as new exploits, vulnerabilities, and technologies are introduced.

MD 12.5 utilizes the policy framework developed by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Standard 27002:2005(E). This framework is broken into 12 primary areas. Each area contains a number of main security categories, which are listed below:

- Access Control
  - Business requirements for access controls - Access control policy.
  - User access managements – User registration, privilege management, user password management, and review of user access rights.

- User responsibilities – Password use, unattended user equipment, and clear desk / screen policy.
- Network access control – Policy on use of network services, user authentication for external connections, equipment identification in networks, remote diagnostic and configuration port protection, segregation in networks, network connection control, and network routing control.
- Operating system access control - Secure log-on procedures; user identification and authentication; password management system; use of system utilities; session time-out; and limitation of connection time.
- Application and information access control – Information access restriction and sensitive system isolation.
- Mobile computing and teleworking – Mobile computing and teleworking policy.

- Asset Management
  - Responsibility for assets - Inventory of assets, ownership of assets, and acceptable use of assets.
  - Information classification - Classification guidelines and information labeling and handling.
- Business Continuity
  - Security aspects of business continuity management - Including security in the business continuity management process; business continuity and risk assessment; developing and implementing continuity plans; business continuity planning framework; and testing, maintaining and re-assessing business continuity plans.
- Communications and Operations Management
  - Operational procedures and responsibilities - Documented operating procedures; change management; segregation of duties; and separation of development, test, and operational facilities.
  - Third party service delivery management - Service delivery; monitoring and review of third party services; and managing changes to third party services.
  - System planning and acceptance - Capacity management and system acceptance.
  - Protection against malicious and mobile code- Controls against malicious code and controls against mobile code.
  - Backup – Information backup.
  - Network security management – Network controls, and security of network services.
  - Media handling - Management of removable media, disposal of media, information handling procedures, and security of system documentation.
  - Exchange of information – Information exchange policies and procedures; exchange agreements; physical media in transit; electronic messaging; and business information systems.
  - Electronic commerce services - Electronic commerce, on-line transactions, and publicly available information.

- Monitoring - Audit logging; monitoring system use; protection of log information; administrator and operator logs; fault logging; and clock synchronization.

- Compliance
  - Compliance with Legal Requirements - Identification of applicable legislation; intellectual property rights (IPR); protection of organizational records; data protection and privacy of personal information; prevention of misuse of information processing facilities; and regulation of cryptographic controls.
  - Compliance with Policies, Standards, and Guidance - Compliance with security policies and standards and technical compliance checking.
  - Information System Audit Considerations - Information systems audit controls and protection of information systems audit tools.
- Human Resource Security
  - Prior to employment – Roles and responsibilities; screening; and terms and conditions of employment.
  - During employment – Management responsibilities; security awareness; education and training; and disciplinary process.
  - Termination or change of employment - Termination responsibilities, return of assets, and removal of access rights.
- Incident Management
  - Reporting security events and weaknesses - Reporting security events and reporting security weaknesses.
  - Management of security incidents and improvements - Responsibilities and procedures; learning from security incidents; and collection of evidence.
- Information Systems Acquisition, Development, and Maintenance
  - Cyber security requirements for information systems – Cyber security requirements analysis and specification.
  - Correct processing in applications – Input data validation, control of internal processing, message integrity, and output data validation.
  - Cryptographic controls – Policy on the use of cryptographic controls and key management.
  - Security of system files – Control of operational software, protection of system test data, and access control to program source code.
  - Security in development and support processes – Change control procedures, technical review of applications after operating system changes, restrictions on changes to software packages, information leakage, and outsourced software development.
  - Technical vulnerability management - Control of technical vulnerabilities.
- Organization
  - Internal – Management commitment to cyber security, cyber security coordination, allocation of cyber security responsibilities, authorization process for information

processing facilities, confidentiality agreements, contact with authorities, contact with special interest groups, and independent review of cyber security.

  - External – Identification of risks related to external parties, addressing security when dealing with customers, and addressing security in third party agreements.

- Physical and Environmental Security
  - Secure areas – Physical security perimeter; securing offices, rooms, and facilities; protecting against external and environmental threats; working in secure areas; and public access, delivery, and loading areas.
  - Equipment security – Equipment siting and protection; supporting utilities; cabling security; equipment maintenance; security of equipment off-premises; secure disposal or re-use of equipment; and removal of property.
- Risk Assessment
  - Assessing security risks
  - Treating security risks
- Security Policy
  - Security policy document
  - Review security policy

7.7.2 Processes, Procedures, Templates, Checklists, Standards, and Guidance

The Contractor shall develop processes, procedures, templates, checklists, standards, and guidance to support the establishment and maintenance of NRC's Cyber Security Program. Each document must comply with the required format for the document type. The required format is provided on the applicable CSO internal web page. The Contractor is expected to establish and maintain documents that will focus on the following aspects of the program:

- Access Control
- Security Awareness and Training
- Auditing and Accountability
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System Services and Acquisition
- System and Communications Protection
- System and Information Integrity

These documents must take into account the following:

- Different types of information systems that the NRC utilizes:
  - Publicly facing systems
  - Large enterprise systems
  - Small systems supporting specific business needs
  - Legacy systems that are beyond their life cycle
  - Systems supporting new technologies
- Information sensitivities for confidentiality, integrity, and availability (FIPS 199 for unclassified systems, CNSS and DNI levels for classified systems)
- Different types of information that the NRC must protect:
  - Unclassified Non-Safeguards Information
  - SGI
  - Classified Information

7.7.3 Security Relevant Business Solutions

The Contractor shall identify and document technical electronic processing solutions that enable secure NRC business processes. These technical solutions may include introduction of new technology or may alter current electronic processing methods for security reasons and may result in more efficient processing. The business solutions shall be documented as NRC Cyber Security standards, processes, procedures, templates, and/or checklists, and shall provide sufficient information for implementation by technically knowledgeable individuals.

8 IT CYBER SECURITY REQUIREMENTS – GENERAL

8.1 Basic Contract Cyber 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 NIST SP 800-60 and must be approved by the primary or alternate COR in writing. The Contractor shall notify the primary and alternate CORs in writing 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, primary and alternate CORs shall be notified before the Contractor begins to process information at a more restrictive classification level.

All work under this task order shall comply with the latest version of all applicable guidance and standards. These standards include, but are not limited to, NRC Management Directive (MD) volume 12 Security, Cyber Security policies issued until MD 12.5, NRC Cyber Security Program is updated, 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 CNSS publications, 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 personnel must sign the NRC Agency Rules of Behavior for Secure Computer Use prior to being granted access to NRC computing resources.

The Contractor shall adhere to following NRC policies:

- NRC Management Directives
- NRC Sensitive Unclassified Non-Safeguards Information (SUNSI)
- Cyber Security Policy for Encryption of Data at Rest When Outside of Agency Facilities
- Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information
- Cyber Security Information Protection Policy
- Remote Access Policy
- Use of Commercial Wireless Devices, Services and Technologies Policy
- Laptop Security Policy
- Cyber Security Incident Response Policy

Contractor shall 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.

8.2 Contract Performance and Completion

The Contractor shall ensure that the NRC data processed during the performance of this task order is purged from all data storage components of the Contractor's computer facility. Tools used to perform data purging shall be approved by the primary or alternate CORs in writing. 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 personnel no longer require access to an NRC system, the Contractor shall notify the primary and alternate CORs within 24 hours.

Upon task order completion, the Contractor shall provide a status list of all NRC system users 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.

8.2.1 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 task order 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.

8.3 Access Controls

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

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

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 National Security Agency (NSA) approved encryption and adhere to guidance in MD 12.2 NRC Classified Information Security Program, MD 12.5 NRC Automated Information Security Program and Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing.

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

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

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

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

8.4 Configuration Standards

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

8.5 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 the primary and alternate CORs for destruction.

8.6 Vulnerability Management

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

- Five (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:

- One (1) calendar day for a high sensitivity system
- Three (3) calendar days for a moderate sensitivity system
- Seven (7) calendar days for a low sensitivity system

9 CORRECTIVE ACTIONS

Issues requiring corrective action shall be identified in a Contract Discrepancy Report (CDR) issued by the primary or alternate CORs. Compliance will be monitored by the NRC through Draft Deliverables, Final Deliverables, Project Schedules, Progress Reports, and primary and alternate COR review of related NRC Customer Satisfaction Surveys.

i.	Target:	Three (3) business days of the CDR issuance meeting
ii.	Data Source:	Draft Deliverables, Final Deliverables, Project Schedules, Progress Reports, and NRC Project Officers reviews of related NRC Customer Satisfaction Surveys
iii.	Frequency:	As needed upon issuance of a CDR
iv.	Exceptions:	The duration will be determined from the time of CDR issuance meeting. The three (3) business day corrective action time will not include time in which the Contractor is waiting on the NRC for data necessary to perform the corrective action.

10 DELIVERABLE STANDARDS

The following standards shall be enforced for all deliverables developed under this task order.

10.1 Deliverable File Formats

The Contractor shall provide all documentation to the primary and alternate CORs electronically via electronic mail in all the following formats, except as specifically stated herein: Microsoft Word (version 2010), Microsoft Excel (version 2010), Microsoft Project (version 2010), and Adobe PDF. All electronic mail shall be transmitted using the Contractor's NRC electronic mail account. Personal and corporate electronic mail accounts shall not be used to transmit or to receive sensitive NRC information.

10.2 Standard for Grammar and Mechanics

All documentation submitted by the Contractor shall conform to the Chicago Manual of Style, as amended by any applicable NRC format templates and requirements.

10.3 Draft and Final Submission

All task order deliverables submitted to the primary and alternate CORs must conform to the standards referenced in this SOW and will be reviewed by the primary and alternate CORs for acceptability.

All documentation shall be submitted in draft form for comment to the primary and alternate CORs. The primary or alternate CORs will be given ten up to (10) business days to generate comments and submit them in writing to the Contractor. Once the Contractor receives the primary or alternate COR's written comments, the Contractor shall have three (3) business days to generate the final draft version of the document. Then, the final draft shall be sent to the primary or alternate CORs for review and approval. Once the final draft has been accepted by the primary or alternate CORs, the Contractor will be given one (1) business day to revise the document. This constitutes a revision cycle.

The first revision cycle for a deliverable shall be acceptable to the Government when the Contractor submits a revised deliverable incorporating any comments and suggestions made by the primary or alternate CORs.

The following provisions also apply to all deliverables:

- Publication of Results: Prior to any dissemination, display, publication or release of articles, reports, summaries, data or related documents developed under the contract, the Contractor shall submit for review and approval by the Contracting Officer the proposed articles, reports, summaries, data and related documents that the Contractor intends to release, disseminate or publish to other persons, the public or any other entities. The Contractor 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 Contracting Officer for release, display, dissemination or publication. The Contractor 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 intends to release, display, disseminate or publish to other persons, the public or any other entities.
- Identification/ Marking of Sensitive and SAFEGUARDS Information: The decision, determination or direction by the COR that information constitutes sensitive or SAFEGUARDS information remains exclusively a matter within the authority of the COR to make. In performing this task order, the Contractor shall clearly mark sensitive unclassified non-SAFEGUARDS information (SUNSI), sensitive, and SAFEGUARDS information to include for example Official Use Only and SAFEGUARDS 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 COR, the Contractor shall use the applicable NRC cover sheet forms (e.g. NRC Form 461 SAFEGUARDS Information and NRC Form 190B Official Use Only) in maintaining these records and documents. The Contractor shall ensure that sensitive and SAFEGUARDS information is handled appropriately, maintained and protected from unauthorized disclosure. The Contractor 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), and NRC Management Directive and Handbook 12.6.
- 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 COR's directions may result in suspension, withholding or offsetting of any payments invoiced or claimed by the Contractor. If the Contractor intends to enter into any subcontracts or other agreements to perform this contract, the Contractor shall include all the above provisions in this Section 11.3 of the SOW in any subcontract or agreements.

10.4 Deliverable Reviews

Deliverable Reviews will be held to provide the Contractor with feedback related to improving the quality of deliverables, including feedback received from Customer Satisfaction Surveys. Such reviews will be coordinated by the primary or alternate CORs as required to supplement written comments provided on deliverable submissions. The written minutes of all deliverable review meetings shall be prepared by the Government. Should the Contractor not concur with the minutes, the Contractor shall so state any areas of non-concurrence in writing to the primary or alternate CORs in writing within 10 calendar days of receipt of the minutes.

11 REPORTING REQUIREMENTS

The Contractor must meet the following reporting requirements.

11.1 Bi-Weekly Funding Report

The bi-Weekly Funding Reports must be submitted to the primary and alternate CORs no later than close of business Tuesday. Bi-Weekly Funding Reports shall cover all Contractor activity that occurred during the previous two (2) calendar weeks.

Bi-Weekly Funding Reports shall identify spending at the 2nd level of the WBS. For each activity being performed under the contract, the following information will be reported.

- Office – Name of the sponsoring office.
- Activity – Name of the activity being performed.
- Budget – Funds obligated to support the activity.
- Money Spent – Amount of funds used to date.
- Money Remaining – Amount of funds remaining.
- Remaining Labor – Amount of funds remaining for labor.
- Remaining ODC – Amount of funds remaining for other than direct cost items like travel

11.2 Monthly Progress Report

Monthly Progress Reports must be submitted to the primary and alternate CORs no later than close of business on the 5th business day of the month. Monthly Progress Reports shall cover all Contractor activity that occurred during the previous month. Monthly Progress Reports must be submitted on the Contractor's letterhead.

11.3 Other Reporting Requirements

The Contractor shall bring problems or potential issues affecting performance to the attention of the primary and alternate CORs and Contracting Officer as soon as possible. Verbal reports shall be followed up with written reports and meetings.

12 MEETINGS

The following meetings will be required under this task order:

- Post Award Conference

The Government will schedule a kick-off meeting once the Contractor's designated personnel have received their security clearance authorization. The NRC will provide an agenda prior to the meeting. The Contractor shall participate in the meeting to establish processes, procedures, and priority of tasking. The Contracting Officer and the primary or alternate CORs will represent the Government. The Contractor shall have equivalent representation at the meeting. The Contractor will be responsible for taking the minutes of this meeting. The minutes will be documented using Microsoft Word. The Contractor must send the minutes to the primary and alternate CORs for their review and approval within three (3) business days.

- Bi-Weekly Meetings (first six (6) months)

  During the first six (6) months of the contract, the Contractor shall meet with the primary or alternate CORs every two (2) weeks to discuss concerns or challenges that are currently being experienced on the contract. The primary and alternate CORs, and Contractor, shall jointly develop the agenda to ensure issues are addressed, deadlines are known, and direction can be provided to resolve any known issues. The Contractor shall be responsible for taking the minutes of this meeting. The minutes will be documented using Microsoft Word. The Contractor must send the minutes to the primary and alternate CORs for their review and/or approval within three (3) business days.

- Monthly Meetings (monthly)

  After six (6) months, the Contractor shall meet with the primary or alternate CORs monthly to discuss concerns or challenges that are currently being experienced on the contract. The primary or alternate CORs and the Contractor shall jointly develop the agenda to ensure issues are addressed, deadlines are known, and direction can be provided to resolve any known issues. The Contractor will be responsible for taking the minutes of this meeting. The minutes shall be documented using Microsoft Word. The Contractor must send the minutes to the primary and alternate CORs for review and/or approval within three (3) business days.

- Ad Hoc Meetings

  Either party may request an ad hoc meeting. The calling party must provide an agenda and a summary description of what is to be discussed 48 business hours before the meeting is held. The Contractor will be responsible for taking the minutes of this meeting. The minutes shall be documented using Microsoft Word. The Contractor must send the minutes to the primary and alternate CORs for their review and/or approval within three (3) business days.