NRC FORM 464 Part I (04-2018) | U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) REQUEST

NRC	RESPONSE NUMBER
2018-000524	1

RESPONSE TYPE ☐ INTERIM ☑ FINAL

REQUESTER:	DATE:
Carina Ice	05/18/2018

DESCRIPTION OF REQUESTED RECORDS:

In relation to contract NRCHQ1014T0001 held by contractor MAR, Inc., with period of performance 02/21/2014 to 05/20/2022: all solicitation documents, all solicitation amendments, and any Q&A from the solicitation period

PART I. -- INFORMATION RELEASED

☐ The NRC has made some, or all, of the requested records publicly available through one or more of the following means: (1) https://www.nrc.gov; (2) public ADAMS, https://www.nrc.gov/reading-rm/adams.html; (3) microfiche available in the NRC Public Document Room; or FOIA Online, https://foiaonline.regulations.gov/foia/action/public/home.

☑ Agency records subject to the request are enclosed.

☐ Records subject to the request that contain information originated by or of interest to another Federal agency have been referred to that agency (See Part I.D -- Comments) for a disclosure determination and direct response to you.

☐ We are continuing to process your request.

☐ See Part I.D -- Comments.

PART I.A -- FEES

AMOUNT
$56.36

☑ You will be billed by NRC for the amount indicated.

☐ You will receive a refund for the amount indicated.

☐ Fees waived.

☐ Since the minimum fee threshold was not met, you will not be charged fees.

☐ Due to our delayed response, you will not be charged fees.

PART I.B -- INFORMATION NOT LOCATED OR WITHHELD FROM DISCLOSURE

☐ We did not locate any agency records responsive to your request. *Note*: Agencies may treat three discrete categories of law enforcement and national security records as not subject to the FOIA ("exclusions"). See 5 U.S.C. 552(c). This is a standard notification given to all requesters; it should not be taken to mean that any excluded records do, or do not, exist.

☐ We have withheld certain information pursuant to the FOIA exemptions described, and for the reasons stated, in Part II.

☐ Because this is an interim response to your request, you may not appeal at this time. We will notify you of your right to appeal any of the responses we have issued in response to your request when we issue our final determination.

☐ You may appeal this final determination within 90 calendar days of the date of this response. If you submit an appeal by mail, address it to the FOIA Officer, at U.S. Nuclear Regulatory Commission, Mail Stop T-2 F43, Washington, D.C. 20555-0001. You may submit an appeal by e-mail to FOIA.resource@nrc.gov. You may fax an appeal to (301) 415-5130. Or you may submit an appeal through FOIA Online, https://foiaonline.regulations.gov/foia/action/public/home. Please be sure to include on your submission that it is a "FOIA Appeal."

PART I.C -- REFERENCES AND POINTS OF CONTACT

You have the right to seek assistance from the NRC's FOIA Public Liaison by submitting your inquiry at https://www.nrc.gov/reading-rm/foia/contact-foia.html, or by calling the FOIA Public Liaison at (301) 415-1276.

If we have denied your request, you have the right to seek dispute resolution services from the NRC's Public Liaison or the Office of Government Information Services (OGIS). To seek dispute resolution services from OGIS, you may e-mail OGIS at ogis@nara.gov, send a fax to (202) 741-5789, or send a letter to: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740-6001. For additional information about OGIS, please visit the OGIS website at https://www.archives.gov/ogis.

NRC FORM 464 Part I
(04-2018)

U.S. NUCLEAR REGULATORY COMMISSION

RESPONSE TO FREEDOM OF INFORMATION ACT (FOIA) REQUEST

NRC	RESPONSE NUMBER
2018-000524	1

RESPONSE TYPE ☐ INTERIM ☑ FINAL

PART I.D -- COMMENTS

Signature - Freedom of Information Act Officer or Designee

Stephanie A. Blaney

Digitally signed by Stephanie A. Blaney
Date: 2018.05.18 09:58:58 -04'00'

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
1		NRC-HQ-R-33-0067	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jordan Pulaski Mail Stop: TWB-01-B10M Washington, DC 20555	3100	U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	3100

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
To all Offerors/Bidders		NRC-HQ-12-R-33-0067
	X	9B. DATED (SEE ITEM 11) 06-01-2012
		10A. MODIFICATION OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [X] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

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

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

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

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

Please see the attached responses to questions.

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Joseph Widdup	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

RFP Reference	Amendment
RFP Section B.1, PRICE/COST SCHEDULE	All occurrences in the solicitation of TMM are amended to read T&M (Time-and-Materials).
RFP Section E.9, ADDENDUM TO PROVISION 52.212-1, page E-5	Under the section **CONTENTS OF NON-COST/PRICE PORTION OF THE PROPOSAL, 2. PERSONNEL QUALIFICATIONS**, the first sentence is amended as follows. FROM: "For each person proposed to work as a direct charge under this task order, the Offeror shall provide a resume not to exceed five pages in length." TO: "For each person proposed as Key Personnel under this task order, the Offeror shall provide a resume not to exceed five pages in length. The resume shall include their name, their proposed GSA Alliant Small Business GWAC labor category, their education, their experience, any applicable professional certifications, their current country of citizenship and the company name of their current employer (if applicable)."
RFP Section E.10 Evaluation—Commercial Items, page E-6	Under the section **Evaluation—Commercial Items, Part (a), Subpart** 2. **PERSONNEL QUALIFICATIONS**, the last sentence is amended as follows. FROM: "The Government will evaluate the extent to which the proposed resumes demonstrate adequate or better qualifications to satisfy (a) the minimum qualifications for the applicable GSA Alliant Small Business GWAC labor category qualifications and (b) the intended contribution to satisfy the requirements of the statement of work." TO: "The Government will evaluate (a) the extent to which the proposed resumes of key personnel demonstrate adequate or better qualifications to satisfy the minimum qualifications for the applicable GSA Alliant Small Business GWAC labor categories; and (b) the extent to which the proposed labor category mix could reasonably be expected to adequately address the requirements of the solicitation." Note, in this RFP, Key Personnel includes supervisory personnel or leaders that will be directly engaged in task order performance and any senior-level subject matter experts that are proposed to be engaged in task order performance.

RFP Reference	Amendment
RFP Section E.10 Evaluation—Commercial Items, page E-7	Under the section **Evaluation—Commercial Items, Part (a), Subpart** 4. **PAST PERFORMANCE INFORMATION**, the last sentence is amended as follows. FROM: "The evaluation may also take into account past performance information regarding predecessor companies, key personnel who have relevant experience, or subcontractors that will perform major or critical aspects of the requirement when such information is relevant to the instant acquisition." TO: "The evaluation may also take into account past performance information regarding predecessor companies, key personnel who have relevant experience, or subcontractors that are proposed to perform major or critical aspects of the requirement when such information is relevant to the instant acquisition. In this RFP, Key Personnel includes supervisory personnel or leaders that will be directly engaged in task order performance and any senior-level subject matter experts that are proposed to be engaged in task order performance."
ATTACHMENT A SOW, Section 4, PERIOD OF PERFORMANCE	Section 4, PERIOD OF PERFORMANCE, of the SOW is amended to read "The base period of performance for this task order is twelve (12) months from date of award. There are seven one-year options and 1 three-month option that may be exercised in accordance with FAR clause 52.217-9."
ATTACHMENT D - PRICE SCHEDULE	ATTACHMENT D - PRICE SCHEDULE is amended to add CLIN 0020 for Other Direct Costs (to include Travel and other items). This CLIN has a plug-in not-to-exceed estimate for that CLIN of $160,000.00 per year. The Offeror shall include that amount in its proposal. See the revised PRICE SCHEDULE attached.
Attachment F, PAST PERFORMANCE QUESTIONNAIRE, page 1	The first sentence in the first paragraph for OFFERORS is deleted and replaced with the following: "Complete sections I and II of this questionnaire for each company, contractor, subcontractor, entity, or team member for which you are submitting past performance information (see solicitation Sections E-9 and E-10)."

RFP Reference	Question	Response
Section 8.6.1 of the SOW, Incident Response Training	How many people are to be trained AND what is the training cycle?	The Incident Response Training will be limited to the internal incident response team. The training is considered to be an inherent part of the IR response team to ensure that the team keeps up to date with regulations and best practices considering cyber security incident response. The company awarded the contract will serve as part of that response team and the training cycle is part of the team's IR process review and update.
Bottom of first page of the SOW	Does the item about a "Cyber Security Laboratory" on the bottom of the first page of the SOW relate to any other section of the SOW?	The Cyber Security Laboratory allows the CSO to support Situational Awareness specific training, testing and simulation. The laboratory is run by another contract, but the NRC plans to have both the CSPSS and the existing vendor to work together in leveraging laboratory resources to support the CSO mission and objectives.
Section 8.6.2 of the SOW, NRC Enterprise Security Architecture	Is there an existing as-is architecture, to-be architecture, transition strategy/roadmap? If so, what tools were used to build them (i.e. System Architect, Enterprise Architect, Rational...)?	The NRC has an existing level of effort to collect, update and revise the enterprise security architecture. The CSO is open to the use of automated tools and would anticipate that vendors would provide tool recommendations as part of their response to this RFP.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
A002		NRC-HQ-R-33-0067	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jordan Pulaski Mail Stop: TWB-01-B10M Washington, DC 20555	3100	U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	3100

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
To all Offerors/Bidders		NRC-HQ-12-R-33-0067
	X	9B. DATED (SEE ITEM 11) 06-05-2012
		10A. MODIFICATION OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [X] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

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

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

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

Please see the attached amendments to the RFP and responses to questions.

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Joseph Widdup	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
A003		NRC-HQ-R-33-0067	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jordan Pulaski Mail Stop: TWB-01-B10M Washington, DC 20555	3100	U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	3100

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
To all Offerors/Bidders		NRC-HQ-12-R-33-0067
	X	9B. DATED (SEE ITEM 11) 05-31-2012
		10A. MODIFICATION OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [X] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

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

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

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

The due date for proposals, specified in box 8 of the RFP cover page (SF 1449), is extended to:

June 27, 2012 by 4:00 P.M.

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Joseph Widdup	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
A004		NRC-HQ-R-33-0067	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
U.S. Nuclear Regulatory Commission Div. of Contracts Attn: Jordan Pulaski Mail Stop: TWB-01-B10M Washington, DC 20555	3100	U.S. Nuclear Regulatory Commission Div. of Contracts Mail Stop: TWB-01-B10M Washington, DC 20555	3100

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
To all Offerors/Bidders		NRC-HQ-12-R-33-0067
	X	9B. DATED (SEE ITEM 11) 05-31-2012
		10A. MODIFICATION OF CONTRACT/ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

[X] The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers [ ] is extended, [X] is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required) N/A.

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

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

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

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

If the GSA eBuy site cannot handle the file size of an offeror's proposal, offeror's may alternatively submit their proposals directly to jordan.pulaski@nrc.gov with the subject line "NRC-HQ-12-R-33-0067 Proposal."

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Joseph Widdup	
15B. CONTRACTOR/OFFEROR _____ (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA BY _____ (Signature of Contracting Officer)	16C. DATE SIGNED

U.S. NUCLEAR REGULATORY COMMISSION

Cyber Security Program Support Services (CSPSS)

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.

A Contracting Officer's Representative (COR) shall be assigned to each activity sponsored by an NRC Office. The Office COR shall be assigned at level one of the Work Breakdown Structure.

A CSO COR shall be assigned to each activity based on the CSO team that is responsible for the effort (FISMA Compliance and Oversight Team (FCOT), Cyber Situational Awareness Team (CSA), Policy Standards and Training Team (PSTT). This assignment will occur at level two of the Work Breakdown Structure.

2 CONTRACT TYPE

This task order will utilize the firm–fixed-price (FFP) and time-and-materials (T&M).

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 PERIOD OF PERFORMANCE

The base period of performance for this task order is twelve (12) months from date of award. There are six one year options that may be exercised in accordance with FAR clause 52.217-9.

5 FACILITY ACCESS

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

5.1 Hours of Operation

The Contractor shall have access to all NRC facilities five (5) days per week, Monday through Friday local time from 6:00 a.m. to 6:00 p.m., 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 24 hours. This shall be addressed on a case by case basis.

5.2 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 COR in writing to process NRC information.

6 TRAVEL

The task order contains the following travel requirements:

(a.) Local travel expenses shall not be reimbursed by the NRC. On-site parking is not available.

(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 shall 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.

6.1 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 COR or alternate COR. Historically, this has occurred only a couple of times a year.

7 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.

8 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).

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.

8.1 Project Management

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

8.1.1 Quality Assurance Plan

The Contractor shall propose a Quality Assurance Plan for this task order. This plan must be approved in writing by the NRC COR 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 COR or their designee.

8.1.2 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 COR. 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 to develop and maintain the project plan. The project plan shall be provided to the COR on a monthly basis and shall be delivered in conjunction with the Monthly Status Report.

8.2 Special Projects

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

8.2.1 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 COR and their designees 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 COR and their designees.

8.2.2 The Contractor shall give a quarterly risk briefing to the COR and their designees that communicates the results of this assessment to NRC management. 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.

8.2.3 Evaluation of New Technologies

The Contractor may be requested to assist the COR 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.

8.2.4 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 COR. Once the COR has reviewed the white papers and decided upon a course of action, the Contractor may be asked to assist the NRC in incorporating selected recommendations into the NRC Cyber Security Program.

8.3 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).

8.3.1 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 COR 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 COR. The Contractor shall update the system's CP once the CP Test Report has been completed to reflect validated information. The COR or their designee 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.

8.3.2 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.

8.4 Continuous Monitoring Support

The Contractor shall assist the COR 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 COR.

  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 COR.
  - **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 COR for review and comment. The Contractor shall revise and update each deliverable as appropriate based on written COR feedback and provide final versions to the COR.

- 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 COR.

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 COR.

  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.

8.5 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.

8.6 Cyber Situational Awareness

The Contractor shall provide the following services.

8.6.1 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.

8.6.2 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 perform the following work and deliverables in support of this task:

- 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 COR and their designees 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 COR and their designees 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 COR or alternate COR, will be based-lined, and the Contractor shall provide updates to the COR 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 COR and their designees, 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 COR and their designees to discuss items that need improvement.

8.6.3 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.

8.6.4 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 an 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.

8.6.5 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 COR or alternate COR 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 indentifies the automated tools that are going to be used for testing. The tools report must be approved by the COR 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 COR 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 COR. The Contractor will not conduct any testing without written approval from the COR and without being under the COR's observation.

8.6.6 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 COR 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

8.7 Policy, Standards, and Training

The Contractor shall provide the following services.

8.7.1 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

8.7.2 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

8.7.3 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.

8.7.4 Cyber Security Awareness Program

In order to comply with FISMA, the NRC must provide Cyber Security awareness courses to all individuals who have access to NRC information systems or have access to NRC data.

The NRC utilizes computer based security awareness courses to meet this federally mandated requirement. The NRC currently has a computer based security awareness course for general users that is updated annually by a Federal Information Systems Security Line of Business (LOB).

The Contractor shall develop, maintain, and update Cyber Security awareness courses to supplement the LOB general awareness course using current electronic training methods to ensure that federally mandated and NRC defined cyber security requirements are satisfied. The courses shall use current technologies such as those used in the current Federal Information Systems Security LOB for security awareness training and shall operate within the NRC

Learning Management System (LMS). All courses must be Sharable Content Object Reference Model (SCORM) compliant and may be customized to meet the needs of the NRC. An "Awareness" course should be completed by the user in an average time of 1 hour or less (excluding any test).

Course completion tracking shall be maintained by the NRC LMS with reports available on-line and downloadable.

8.7.4.1 Course Descriptions

The NRC General User Awareness course is comprised of federally provided general user awareness content and NRC provided SGI awareness content. Together these convey NRC's Cyber Security relevant requirements for electronic SGI information. The Contractor shall be responsible for ensuring that the NRC SGI content and the federally provided general user awareness content are properly integrated.

. At a minimum, the SGI content shall address the following:

- User Authentication Methods
- End user responsibilities
- Electronic media
- Electronic handling, access and storage
- Use of E-Mail
- Use of mobile devices
- Malicious actor techniques, such as social engineering
- Social networking security considerations

Note: Other topics may be added later as additional requirements become known.

8.7.5 Cyber Security Role-based Training Program

In order to comply with FISMA, the NRC must provide Cyber Security role-based training to all individuals with significant security responsibilities. The Contractor will develop and deliver courses that address all FISMA requirments and ensure all course materials are kept up-to-date.

The NRC role-based training program currently contains the following courses:

- Role-based Training for ISSOs

  This course is for system and office ISSOs and at a minimum covers the following topics:

  - ISSO role in relation to other NRC roles and positions
  - Information technology initiatives
  - ISSO roles and responsibilities
  - Role separation
  - Procurement

- Threats
- Vulnerabilities
- Risk management
- Operational, management, and technical security controls
- Planning
- Site/system security plans
- Authorization to Operate
- Continuous monitoring
- Incident reporting
- Continuity of operations

- Role-based Training for System Administrators of Windows-Based Systems

  This course is for Windows System Administrators and at a minimum covers the following topics:

  - Security configuration guidelines
  - NRC policies and procedures
  - Authorization to Operate
  - Vulnerabilities
  - Threats
  - Auditing
  - Continuous Monitoring
  - Incident response

  Note: A portion of this class is devoted to hands-on exercises that guide students in implementing current security configuration requirements for Microsoft Windows servers and workstations.

- Role-based Training for System Administrators of Linux/Unix-Based Systems

  This course is for Linux/Unix System Administrators and at a minimum covers the following topics:

  - Security configuration guidelines
  - NRC policies and procedures
  - Authorization to Operate
  - Vulnerabilities
  - Threats
  - Auditing
  - Continuous Monitoring

- Incident response

Note: A portion of this class is devoted to hands-on exercises that guide students in implementing current security configuration requirements for Microsoft Windows servers and workstations.

- Role-based Training for Senior IT Managers and System Owners

  This course is for Senior IT Managers and Systems Owners and at a minimum covers the following topics:

  - Federal and NRC policies, guidance, regulations and requirements
  - NRC FISMA results
  - Office of Inspector General (OIG) audits and other NRC auditing or inspection reports
  - Planning
  - Procurement
  - Security in the life-cycle
  - Role separation
  - Risk management
  - System security plans
  - Vulnerabilities
  - Threats
  - Security Controls
  - Authorization to operate
  - Continuous monitoring

- Role-based Training for the DAA

  This course is for individuals with DAA responsibilities and must include information that describes the role and responsibilities for all levels of systems.

  Note: The course topics must be related to NRC examples and designed at a high level to help senior level managers and executives evaluate the components of an IT security program with regard to critical business functions and the NRC's specific IT requirements as well as understand their role as it relates to other NRC roles and positions.

- Role-based Training for Senior Level Managers and Executives

  This course is for Senior Level Managers and Executives and at a minimum covers the following topics:

  - Federal and NRC policies, guidance, regulations and requirements
  - NRC FISMA results
  - Office of Inspector General (OIG) audits and other NRC auditing or inspection reports
  - Overview of the Authorization

- Role separation
- Risk management
- Vulnerabilities
- Threats
- Security Controls
- Authorization to operate

Note: The course topics must be related to NRC examples and designed at a high level to help senior level managers and executives evaluate the components of an IT security program with regard to critical business functions and the NRC's specific IT requirements as well as understand their role as it relates to other NRC roles and positions.

8.7.6 Cyber Security Conference

Upon request of the COR, the Contractor shall support them with the implementation of an annual Cyber Security conference, to include multiple tracks addressing both IT security awareness and in-depth role-based Cyber Security information. The attendees of the conference will be NRC staff and Contractors. Conference duration shall be no more than three (3) days in length. The objective of the conference will be to increase staff knowledge and understanding of Cyber Security.

The Contractor shall provide the staff necessary to run three (3) possibly concurrent conference tracks, for example:

- IT Security for the general user, focusing on understanding the reason for Cyber Security
- IT Security for Cyber Security implementers (e.g., ISSOs, system administrators, developers)
- IT Security for Managers and Executives

A variety of methods and techniques should be used to enable understanding of the message across the conference tracks.

Basic administrative functions for the conference (e.g., arrangement for physical space, physical conference set-up and tear-down) shall be provided using another NRC resource.

8.7.6.1 Place of Performance

The COR will identify the physical location where the Security Conference will be held at least 3 months in advance.

8.7.6.2 Provided Services

The Contractor shall provide trainers in the field of Cyber Security who have experience supporting and providing training in the following areas:

- Operating Systems – VMware, Linux, Solaris 10, Microsoft Windows 7, Microsoft Windows 2008 Servers, Microsoft Windows 2003 Servers, Mac OS.
- Applications - Microsoft Exchange, Microsoft Internet Information Services (IIS), Oracle, Sybase, Citrix, MS SQL Server, MS SharePoint, MS .Net Framework, Apache Web Server,

Social Networking software, Blackberry Enterprise Server and Handheld, and IBM Rational Suite.

- Information Assurance - Network Engineering, Network Monitoring, Active Directory, Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS), Firewalls, Virtual Private Networking (VPN), Public Key Infrastructure (PKI), Wireless, Remote Access Systems (RAS), Malware, Spyware, and Penetration Testing.

8.7.7 Electronically Communicating Cyber Security Information

The Contractor shall work with the COR to enhance user knowledge of Cyber Security. This effort will focus on raising the level of Cyber Security understanding of all NRC staff and Contractors. The Contractor shall develop a monthly security news letter that summarizes changes in policies and requirements and keeps the reader apprised of the current risks and threats that are being seen inside and outside the NRC.

The Contractor shall review the security awareness program annually and provide recommendations to the NRC on how the program can be more effective and reach a wider audience.

The Contractor shall assist the CSO in establishing and maintaining their web site.

9 IT CYBER SECURITY REQUIREMENTS – GENERAL

9.1 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 CSO in writing. The Contractor shall notify the COR 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 and Project Officers 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.

9.2 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 COR 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 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.

9.2.1 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.

9.3 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.

9.4 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.

9.5 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 COR for destruction.

9.6 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

10 CORRECTIVE ACTIONS

Issues requiring corrective action shall be identified in a Contract Discrepancy Report (CDR) issued by the COR. Compliance will be monitored by the NRC through Draft Deliverables, Final Deliverables, Project Schedules, Progress Reports, and 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.

11 DELIVERABLE STANDARDS

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

11.1 Deliverable File Formats

The Contractor shall provide all documentation to the COR electronically via electronic mail in all the following formats, except as specifically stated herein: Microsoft Word (version 2007), Microsoft Excel (version 2007), Microsoft Project (version 2007), 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.

11.2 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.

11.3 Draft and Final Submission

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

All documentation shall be submitted in draft form for comment to the COR. The COR 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 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 COR for review and approval. Once the final draft has been accepted by the COR, 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 COR.

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.

11.4 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 COR 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 COR in writing within 10 calendar days of receipt of the minutes.

12 REPORTING REQUIREMENTS

The Contractor must meet the following reporting requirements.

12.1 Bi-Weekly Funding Report

The bi-Weekly Funding Reports must be submitted to the COR 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

12.2 Monthly Progress Report

Monthly Progress Reports must be submitted to the COR no later than close of business on the 5th calendar 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. These reports must contain the information specified in Attachment 1 – Monthly Progress Report Format.

12.3 Other Reporting Requirements

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

13 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 COR 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 COR 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 NRC every two (2) weeks to discuss concerns or challenges that are currently being experienced on the contract. The COR and their designees, 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 COR for their review and approval within three (3) business days.

- Monthly Meetings (monthly)

  After six (6) months, the Contractor shall meet with the NRC monthly to discuss concerns or challenges that are currently being experienced on the contract. The COR 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 COR for approval within three (3) business days.

- Ad Hoc Meetings

  Either party may request an adhoc 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 COR for their review and approval within three (3) business days.

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

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

The contractor shall prepare vouchers/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

Form: Claims shall be submitted on the payee's letterhead, voucher/invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal--Continuation Sheet."

Number of Copies: A signed original shall be submitted. If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original is also required.

Designated Agency Billing Office: The preferred method of submitting vouchers/invoices is electronically to the Department of the Interior at NRCPayments@nbc.gov

If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be electronically sent to: Property@nrc.gov

However, if you submit a hard-copy of the voucher/invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

If you submit a hard-copy of the voucher/invoice and it includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be mailed to the following address:

U.S. Nuclear Regulatory Commission
NRC Property Management Officer
Mail Stop: O-4D15
Washington, DC 20555-0001

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of Standard Form 26, Block 25 of Standard Form 33, or Block 18a. of Standard Form 1449, whichever is applicable.

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

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

Format: Claims shall be submitted in the format depicted on the attached sample form entitled "Voucher/Invoice for Purchases and Services Other than Personal" (see Attachment 1). The sample format is provided for guidance only. The format is not required for submission of a voucher/invoice. Alternate formats are permissible provided all requirements of the billing instructions are addressed.

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

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

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

Supersession: These instructions supersede any previous billing instructions.

R:txtselden\billing instructions LH or TM revised 2008

BILLING INSTRUCTIONS FOR LABOR HOUR/TIME AND MATERIALS TYPE CONTRACTS (JUNE 2008) INVOICE/VOUCHER FOR PURCHASES AND SERVICES OTHER THAN PERSONAL (SAMPLE FORMAT - COVER SHEET)

1. Official Agency Billing Office

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

2. Voucher Information

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

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

c. Contract Number. Insert the NRC contract number.

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

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

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

g. Required Attachments (Supporting Documentation). Direct Costs. The contractor shall submit as an attachment to its invoice/voucher cover sheet a listing of labor categories, hours billed, fixed hourly rates, total dollars, and cumulative hours billed to date under each labor category authorized under the contract/purchase order for each of the activities to be performed under the contract/purchase order. The contractor shall include incurred costs for: (1) travel, (2) materials, including non-capitalized equipment and supplies, (3) capitalized nonexpendable equipment, (4) materials handling fee, (5) consultants (supporting information must include the name, hourly or daily rate of the consultant, and reference the NRC approval), and (6) subcontracts (include separate detailed breakdown of all costs paid to approved subcontractors during the billing period) with the required supporting documentation, as well as the cumulative total of each cost, billed to date by activity.

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

3. Definitions

a. Non-capitalized Equipment, Materials, and Supplies. These are equipment other than that described in number (4) below, plus consumable materials, supplies. List by category. List items valued at $1,000 or more separately. Provide the item number for each piece of equipment valued at $1,000 or more.

b. Capitalized Non Expendable Equipment. List each item costing $50,000 or more and having a life expectancy of more than one year. List only those items of equipment for which reimbursement is requested. For each such item, list the following (as applicable): (a) the item number for the specific piece of equipment listed in the property schedule of the contract; or (b) the Contracting Officer's approval letter if the equipment is not covered by the property schedule.

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

Sample Voucher Information (Supporting Documentation must be attached)

This voucher/invoice represents reimbursable costs for the billing period from _____ through _____.

		Amount Billed Current Period	Cumulative
(f)	Direct Costs:		
	(1) Direct Labor	$_____	$_____
	(2) Travel	$_____	$_____
	(3) Materials	$_____	

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

$____
_____

(4) Equipment

$____
_____
$____
_____

(5) Materials Handling Fee $_____ $_____

(6) Consultants $_____ $_____

(7)
Subcontracts

$____
_____
$____
_____

Total Direct Costs:

$____
_____
$____
_____

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

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

The contractor shall prepare vouchers/invoices as prescribed herein. FAILURE TO SUBMIT VOUCHERS/INVOICES IN ACCORDANCE WITH THESE INSTRUCTIONS WILL RESULT IN REJECTION OF THE VOUCHER/INVOICE AS IMPROPER.

Form: Claims shall be submitted on the payee's letterhead, voucher/invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal--Continuation Sheet."

Number of Copies: A signed original shall be submitted. If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original is also required.

Designated Agency Billing Office: The preferred method of submitting vouchers/invoices is electronically to the Department of the Interior at NRCPayments@nbc.gov

If the voucher/invoice includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be electronically sent to: Property@nrc.gov

However, if you submit a hard-copy of the voucher/invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

If you submit a hard-copy of the voucher/invoice and it includes the purchase of any property with an initial acquisition cost of $50,000 or more, a copy of the signed original shall be mailed to the following address:

U.S. Nuclear Regulatory Commission
NRC Property Management Officer
Mail Stop: O-4D15
Washington, DC 20555-0001

HAND-CARRIED SUBMISSIONS WILL NOT BE ACCEPTED

ATTACHMENT

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

Agency Payment Office: Payment will continue to be made by the office designated in the contract in Block 12 of the Standard Form 26, Block 25 of the Standard Form 33, or Block 18a. of the Standard Form 1449, whichever is applicable.

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

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

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

2. **Contract number.**

3. **Sequential voucher/invoice number.**

4. **Date of voucher/invoice.**

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

6. **A description of articles or services, quantity, unit price, and total amount.**

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

8. **Weight and zone of shipment, if shipped by parcel post.**

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

10. **Instructions to consignee to notify the Contracting Officer of receipt of shipment.**

BILLING INSTRUCTIONS FOR FIXED PRICE CONTRACTS (JUNE 2008)

11. For Indefinite Delivery contracts or contracts under which progress payments are authorized, the final voucher/invoice shall be marked "FINAL VOUCHER" OR "FINAL INVOICE."

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

Supersession: These instructions supersede any previous billing instructions.

R:txtselden\billing instructions FP revised 2008

LIST OF CONTRACT SIMILAR IN SCOPE

1. Firm Name & Address:	2. Year Firm Established:	3. Date Prepared:
	4. Type of Firm: __A. Small Business __B. Small Disadvantaged __C. Woman-Owned __D. Hubzone __E. Service-Disabled Veteran-Owned __F. Other (Specify)_____	
5. Principal Points of Contact: (List two by Name/Title/Current Telephone Number)		
6. Present Offices: (Address/Telephone)		
7. Past Performance Last 3 Years (1) List Contracts Similar in Size (Dollars) and Scope; (2) List Contracts Similar in Scope Only		
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:

NRC-HQ-12-R-33-0067 Attachment E – List of Contracts

Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirements:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:
Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:

Contract No: Period of Performance: Dollar Value: Name of Gov./Commercial Entity:	Contracting Contact Name & Phone: Technical Rep. Name & Phone:	Brief Description and How it is Similar to NRC=s Requirement:

The foregoing is a statement of facts

Signature: _____ Title: _____ Date: _____

Attachment F

PAST PERFORMANCE QUESTIONNAIRE
FOR SOLICITATION NO. NRC-HQ-12-R-33-0067

REQUESTED RESPONSE: In Accordance with each Functional Area Proposal Due date.

EVALUATOR: Please complete questionnaire and email to:
jordan.pulaski@nrc.gov

OFFEROR: Complete sections I and II of this questionnaire for each company, contractor, subcontractor, entity, or team member for which you are submitting past performance information (see solicitation Sections E-9 and E-10). For each contract/order, listed in the response to the RFP, provide one copy of this questionnaire to the Program Manager/Project Manager/COTR and one copy to the Contracts Administrator/Contracting Officer/Contract Specialist of the referenced firm or government agency for completion.

EVALUATOR: Please cross-out and correct any information that is incorrect in Sections I and II, sign the bottom of this page after completing Section II and then email the completed form as indicated in the above box.

I. IDENTIFICATION OF CONTRACTOR BEING EVALUATED [Offeror – complete this section for each contract/order]**:**

1. Company/Division (Contractor) Providing Services: _____
2. Address: _____
3. Contract/Order Number: _____ Dollar Value (Total (if all options exercised) and Total to date): _____
4. Performance Period: _____ Performance Location: _____
5. Type of Contract (Check One):

Fixed Price _____ Cost Reimbursement _____ Other (specify type) _____

6. Basis of Award (Check One):

Competitive _____ Non-Competitive _____

7. Describe Type and Extent of Subcontracting (if any):

II. EVALUATED BY [Offeror – complete this Section; Evaluator - please correct any misinformation and sign]**:**

Company/Organization Name: _____

Company/Organization Address: _____

Evaluator's Name and Title: _____

Evaluator's Signature: _____ Date: _____

Email : _____ Phone: _____

Attachment F

PAST PERFORMANCE QUESTIONNAIRE
FOR SOLICITATION NO. NRC-HQ-12-R-33-0067

Evaluator: Please answer questions 1 through 13 (below) using the following criteria. Circle only one response per question. For questions rated 1 (Marginal) or 0 (Unsatisfactory), please comment on the specific problem(s) or performance failure(s) that prompted this rating.

4 – Excellent - Performance met and exceeded many of the contractual requirements to the organization's benefit. The contractual performance of the element being evaluated was accomplished with few or no minor problems for which corrective actions were highly effective.

3 - Very Good - Performance met and exceeded some of the contractual requirements to the organization's benefit. The contractual performance of the element being evaluated was accomplished with some (or few or no) minor problems for which corrective actions were effective.

2 – Satisfactory - Performance met contractual requirements. The contractual performance of the element being evaluated was accomplished with some minor problems for which corrective actions were satisfactory.

1 – Marginal - Performance barely met contractual requirements. The contractual performance of the element being evaluated reflects problems, for which corrective actions have not yet been identified, appear only marginally effective or was not fully implemented.

0 – Unsatisfactory - Performance did not meet some contractual requirement and recovery is not likely in a timely manner. The contractual performance of the element being evaluated reflects serious problems for which corrective actions were ineffective.

N/A - Not applicable or not observed.

1. Rate the contractor's overall commitment to quality performance and customer satisfaction.

4 3 2 1 0 N/A

Comment:

2. Rate the contractor's overall technical competence.

4 3 2 1 0 N/A

Comment:

PAST PERFORMANCE QUESTIONNAIRE
FOR SOLICITATION NO. NRC-HQ-12-R-33-0067

3. Rate the contractor's cooperation and willingness to work as a team (with your personnel, other contractors, etc.).

4 3 2 1 0 N/A

Comment:

4. Rate the contractor's compliance with contractual requirements.

4 3 2 1 0 N/A

Comment:

5. Rate the contractor's responsiveness to contract changes, changes in technical requirements and/or schedule changes.

4 3 2 1 0 N/A

Comment:

6. Rate the effectiveness of the contractor's overall quality control procedures.

4 3 2 1 0 N/A

Comment:

7. Rate the effectiveness of the contractor's management and supervision.

4 3 2 1 0 N/A

Comment:

PAST PERFORMANCE QUESTIONNAIRE
FOR SOLICITATION NO. NRC-HQ-12-R-33-0067

8. Rate the contractor's ability to overcome technical problems, labor issues, and/or other performance difficulties.

4 3 2 1 0 N/A

Comment:

9. Rate the contractor ability to reframe from unreasonable or excessive change order request.

4 3 2 1 0 N/A

Comment:

10. Rate the contractor's ability to plan and conduct operations in a cost effective manner.

4 3 2 1 0 N/A

Comment:

11. Rate the contractor's ability to adhere to schedules and complete work on time.

4 3 2 1 0 N/A

Comment:

12. Rate the quality and stability of the contractor's workforce utilized on the contract/order.

4 3 2 1 0 N/A

Comment:

13. Rate the availability, adequacy, and suitability of the contractor's staffing for the work required.

4 3 2 1 0 N/A

Comment:

PAST PERFORMANCE QUESTIONNAIRE
FOR SOLICITATION NO. NRC-HQ-12-R-33-0067

14. **Rate the contractor's ability to recruit new personnel for the contract/order within a reasonable period of time**

4 3 2 1 0 N/A

Comment:

Thank you for your assistance in completing this Past Performance Questionnaire.

U.S. Nuclear Regulatory Commission
Division of Contracts

ATTACHMENT I - MONTHLY PROGRESS REPORT FORMAT

A separate monthly progress report shall be created for each NRC Office that has sponsored work under the contract.

GENERAL INFORMATION / DESCRIPTION

- Contractor's Name
- Contractor's Business Address

- Contract name
- Contract number
- Order number

- Billing month the report represents
- Date the report was prepared

- Contractor Program Manager Name
- Contractor Program Manager Telephone Number

- Table of Contents grouped by NRC Office then activity

FINANCIAL SUMMARY

- Total amount of funds obligated
- Total costs incurred during the current reporting period.
- Total amount of money spent to date
- Total amount of money spent this fiscal year
- Percentage of funds expended to date verses the obligated amount

STATUS (Organized by Office, Activity, and Task)

The monthly report will contain a detailed status that identifies by task the costs incurred during the current reporting period.

Activity	Task Name	Scheduled Completion	Status	Task Cost	Travel	Work Performed
Activity 1 (Name)	Task 1 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Activity 1 (Name)	Task 2 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Activity 1 (Name)	Task 3 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Amount of money spent on the activity during the reporting period ($9,999,999.00)						Total Activity 1
Activity 2 (Name)	Task 1 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Activity 2 (Name)	Task 2 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Activity 2 (Name)	Task 3 (Name)	Date when task is scheduled for completion (mm/dd/yyyy)	Task Status (Completed Ongoing Overdue On Hold)	Amount of money spent on supporting the task in the current reporting period ($9,999,999.00)	Amount of money spent travel ($9,999)	Brief description of the work performed during the reporting period
Amount of money spent on the activity during the reporting period ($9,999,999.00)						Total Activity 2

Note: Work Breakdown Structure (WBS) level 1 is the NRC office sponsoring the work. WBS level 2 is the activity being performed by system (Authorization, Continuous Monitoring, etc.) or activities that are being done to directly support the office's Cyber Security Program (Special Projects, Procedures, Supporting Documentation, etc.). WBS level 3 is a breakdown of the activities by task (Security Categorization, System Security Plan, Contingency Plan, Contingency Plan Report, etc.). WBS level 4 would be the major milestones and steps needed to accomplish each task.

EARNED VALUE MANAGEMENT (EVM) DATA

The Contractor shall report earned value consistent with the Section A-11, Part 7 of the ANSI Standard 748. Schedule variance data submitted shall provide visibility into root causes and establish corrective actions to achieve project completion within the established schedule. All EVM data shall be provided in tabular and graphical formats to communicate cost variance and schedule status, as well as the technical completion status of the project relative to the Performance Measurement Baseline.

- EVM data shall be collected at level 2 of the WBS and includes 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, 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 can be integrated with higher-level schedules.
- The Contractor shall collect and report on each of the following measures:
  - Performance Measurement Baseline (PMB)
  - Budget Cost of Work Scheduled (BCWS)
  - Actual Cost of Work Performed (ACWP)
  - Budgeted Cost of Work Performed (BCWP)
  - Cost Variance (CV) – The numerical difference between the earned value (BCWP) and the actual cost (ACWP). CV = BCWP – ACWP.
  - Schedule Variance (SV) - An indicator of how much a program is ahead of or behind schedule. SV = BCWP – BCWS.
  - Cost Performance Index (CPI) – The cost efficiency factor representing the relationship between the actual cost expended and the earned value. CPI = BCWP/ACWP.
  - Schedule Performance Index (SPI) – The planned schedule efficiency factor representing the relationship between the earned value and the initial planned schedule. SPI = BCWP/BCWS.
  - Budget at Completion (BAC) – sum total of the time-phased budget.
  - Estimate to Complete (ETC) – A calculated value, in dollars or hours that represents the cost of work required to complete remaining project tasks. ETC = BAC – BCWP.

- Estimate at Completion (EAC) – A calculated value, in dollars or hours that represents the projected total final costs of work when completed. EAC = ACWP + ETC.

- The Contractor shall calculate Earned value credit as a binary value, with 0 percent being given before task completion and 100 percent given when completion of each work unit is validated. The Contractor shall establish specific measurable exit criteria for each task to simplify tracking of task completion, and thus credit the earned value of the task to the project so that the earned value of the project at any given point in time is obtained by "simple math" rather than by subjective assessment.

PROBLEM/RESOLUTION

All problems encountered during the reporting period should be clearly and sufficiently identified and stated. Then, the resolution or the proposed solution should be briefly described. If the problem still exists in a subsequent month, in whole or in part, it should be described as it currently exists; otherwise, it should be deleted from the report. Problems or circumstances that require a change in the level of effort/costs, scope, or travel requirements are to be described in the Progress Reports for documentation purposes, but are to be dealt with separately in a letter addressed to the Project Officer and Contracting Officer.

PLANS FOR NEXT PERIOD

A brief description that describes the work the contractor is planning to do during the next reporting period. If a milestone is expected to be completed during the next reporting period, identify this milestone.

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NO.	PAGE 1 OF XX

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			NRC-HQ-12-R-33-0067	May 2, 2012

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
			June 15, 2012 4:00 P.M. EST

9. ISSUED BY — CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Jordan Pulaski
Mail Stop: TWB-01-B10M
Washington, DC 20555

10. THIS ACQUISITION IS
- [ ] UNRESTRICTED OR [X] SET ASIDE: 100 % FOR:
- [X] SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] HUBZONE SMALL BUSINESS
- [ ] EDWOSB
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] 8(A)

NAICS: 541519

SIZE STANDARD: $25.5 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING	14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE	N/A	[ ]	N/A	[ ] RFQ [ ] IFB [X] RFP

15. DELIVER TO — CODE

U.S. Nuclear Regulatory Commission

Washington DC 20555

16. ADMINISTERED BY — CODE 3100

U.S. Nuclear Regulatory Commission
Div. of Contracts
Mail Stop: TWB-01-B10M

Washington, DC 20555

17a. CONTRACTOR/OFFEROR CODE ____ FACILITY CODE ____

TELEPHONE NO.

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE 3100

Department of Interior / NBC
NRCPayments_NBCDenver@NBC.gov
Attn: Fiscal Services Branch - D2770
7301 W. Mansfield Avenue
Denver CO 80235-2230

PHONE: FAX:

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED
[ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	The contractor shall provide the U.S. Nuclear Regulatory Commission (NRC) with the services described in the enclosed Statement of Work (SOW) - Attachment A, and terms and conditions of this task order.				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

[X] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED.

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
		Joseph L. Widdup Contracting Officer	

Table of Contents

B.1 PRICE/COST SCHEDULE

The contract type for the items is as follows:

SOW Reference	Category/Item	Contract Type
8.0	Overall Contract Responsibilities	T&M
8.1.2	Project Plan and Project Manager Support	T&M
8.2.1	Residual Risk per system	FFP/TMM
8.2.2	Classified Processing Support	T&M
8.2.3	Evaluate New Technology	T&M
8.2.4	Best Practices	T&M
8.3.1	Authorization	FFP/TMM
8.3.2	Laptop Authorization	FFP
8.4	Continuous Monitoring Support	FFP/TMM
8.5	Data Calls	T&M
8.6.1	Incident Response	T&M
8.6.2	Security Architecture	T&M
8.6.3	Vulnerability Assessment	FFP/TMM
8.6.4	Source Code Reviews	T&M
8.6.5	Penetration Testing	T&M
8.6.6	Security Impact Assessments	FFP/TMM
8.7.1	Cyber Security Policy	T&M
8.7.2	Processes, Procedures, Templates, Checklists, Standards, and Guidance	T&M
8.7.3	Cyber Security Relevant Business Solutions	T&M
8.7.4	Cyber Security Awareness Training	T&M
8.7.5	Cyber Security Role Based Awareness Training (development and instruction)	FFP/TMM
8.7.6	Cyber Security Conference	T&M
8.7.7	Communications	T&M

B.2 BRIEF PROJECT TITLE AND WORK DESCRIPTION (AUG 2011)

(a) The title of this project is:

"CYBER SECURITY PROGRAM SUPPORT SERVICES" (CSPSS)

(b) Summary work description:

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. 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.

B.3 CONSIDERATION AND OBLIGATION--DELIVERY ORDERS (AUG 2011)

(a) The ceiling of this order for services is to be specified at time of award.

(b) Reserved

(c) The amount presently obligated with respect to this order is to be specified at time of award. 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 - 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 work under T&M CLINs.

SECTION C - CONTRACT CLAUSES

C.1 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (FEB 2012)

(a) Inspection/Acceptance. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its post-acceptance rights-

(1) Within a reasonable time after the defect was discovered or should have been discovered; and

(2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) Assignment. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) Changes. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) Disputes. This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) Definitions. The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) Excusable delays. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies(or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer-- Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer--Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) Patent indemnity. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payment.-

(1) Items accepted. Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) Prompt payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) Overpayments. If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall--

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the--

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected contract line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) Interest.

(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in Section 611 of the Contract Disputes Act of 1978 (Public Law 95-563), which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final decisions. The Contracting Officer will issue a final decision as required by 33.211 if--

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on--

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) Risk of loss. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) Taxes. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) Termination for the Government's convenience. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) Termination for cause. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) Title. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) Warranty. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) Limitation of liability. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) Other compliances. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, et seq., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-

Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) Order of precedence. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments

(9) The specification.

(t) Central Contractor Registration (CCR).

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in FAR subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the CCR database; (B) comply with the requirements of subpart 42.12; and (C) agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will

be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via CCR accessed through https://www.acquisition.gov or by calling 1-888-227-2423 or 269-961-5757.

C.2 52.212-4 CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (FEB 2012) ALTERNATE I (OCT 2008)

(a) Inspection/Acceptance.

(1) The Government has the right to inspect and test all materials furnished and services performed under this contract, to the extent practicable at all places and times, including the period of performance, and in any event before acceptance. The Government may also inspect the plant or plants of the Contractor or any subcontractor engaged in contract performance. The Government will perform inspections and tests in a manner that will not unduly delay the work.

(2) If the Government performs inspection or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish and shall require subcontractors to furnish all reasonable facilities and assistance for the safe and convenient performance of these duties.

(3) Unless otherwise specified in the contract, the Government will accept or reject services and materials at the place of delivery as promptly as practicable after delivery, and they will be presumed accepted 60 days after the date of delivery, unless accepted earlier.

(4) At any time during contract performance, but not later than 6 months (or such other time as may be specified in the contract) after acceptance of the services or materials last delivered under this contract, the Government may require the Contractor to replace or correct services or materials that at time of delivery failed to meet contract requirements. Except as otherwise specified in paragraph (a)(6) of this clause, the cost of replacement or correction shall be determined under paragraph (i) of this clause, but the "hourly rate" for labor hours incurred in the replacement or correction shall be reduced to exclude that portion of the rate attributable to profit. Unless otherwise specified below, the portion of the "hourly rate" attributable to profit shall be 10 percent. The Contractor shall not tender for acceptance materials and services required to be replaced or corrected without disclosing the former requirement for replacement or correction, and, when required, shall disclose the corrective action taken. [Insert portion of labor rate attributable to profit.]

(5)(i) If the Contractor fails to proceed with reasonable promptness to perform required replacement or correction, and if the replacement or correction can be performed within the ceiling price (or the ceiling price as increased by the Government), the Government may--

(A) By contract or otherwise, perform the replacement or correction, charge to the Contractor any increased cost, or deduct such increased cost from any amounts paid or due under this contract; or

(B) Terminate this contract for cause.

(ii) Failure to agree to the amount of increased cost to be charged to the Contractor shall be a dispute under the Disputes clause of the contract.

(6) Notwithstanding paragraphs (a)(4) and (5) above, the Government may at any time require the Contractor to remedy by correction or replacement, without cost to the Government, any failure by the Contractor to comply with the requirements of this contract, if the failure is due to--

(i) Fraud, lack of good faith, or willful misconduct on the part of the Contractor's managerial personnel; or

(ii) The conduct of one or more of the Contractor's employees selected or retained by the Contractor after any of the Contractor's managerial personnel has reasonable grounds to believe that the employee is habitually careless or unqualified.

(7) This clause applies in the same manner and to the same extent to corrected or replacement materials or services as to materials and services originally delivered under this contract.

(8) The Contractor has no obligation or liability under this contract to correct or replace materials and services that at time of delivery do not meet contract requirements, except as provided in this clause or as may be otherwise specified in the contract.

(9) Unless otherwise specified in the contract, the Contractor's obligation to correct or replace Government-furnished property shall be governed by the clause pertaining to Government property.

(b) Assignment. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) Changes. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) Disputes. This contract is subject to the Contract Disputes Act of 1978, as amended (41 U.S.C. 601-613). Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) Definitions.

(1) The clause at FAR 52.202-1, Definitions, is incorporated herein by reference. As used in this clause--

(i) Direct materials means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) Hourly rate means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are--

(A) Performed by the contractor;

(B) Performed by the subcontractors; or

(C) Transferred between divisions, subsidiaries, or affiliates of the contractor under a common control.

(iii) Materials means--

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (e.g., incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.);

(D) The following subcontracts for services which are specifically excluded from the hourly rate: [Insert any subcontracts for services to be excluded from the hourly rates prescribed in the schedule.]; and

(E) Indirect costs specifically provided for in this clause.

(iv) Subcontract means any contract, as defined in FAR Subpart 2.1, entered into with a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract including transfers between divisions, subsidiaries, or affiliates of a contractor or subcontractor. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(f) Excusable delays. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) Invoice.

(1) The Contractor shall submit an original invoice and three copies(or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, contract line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer-- Central Contractor Registration, or

52.232-34, Payment by Electronic Funds Transfer--Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) Patent indemnity. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) Payments.

(1) Services accepted. Payment shall be made for services accepted by the Government that have been delivered to the delivery destination(s) set forth in this contract. The Government will pay the Contractor as follows upon the submission of commercial invoices approved by the Contracting Officer:

(i) Hourly rate.

(A) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the contract by the number of direct labor hours performed. Fractional parts of an hour shall be payable on a prorated basis.

(B) The rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by individuals that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(C) Invoices may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer) to the Contracting Officer or the authorized representative.

(D) When requested by the Contracting Officer or the authorized representative, the Contractor shall substantiate invoices (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment, individual daily job timecards, records that verify the employees meet the qualifications for the labor categories specified in the contract, or other substantiation specified in the contract.

(E) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis.

(1) If no overtime rates are provided in the Schedule and the Contracting Officer approves overtime work in advance, overtime rates shall be negotiated.

(2) Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract.

(3) If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(ii) Materials.

(A) If the Contractor furnishes materials that meet the definition of a commercial item at FAR 2.101, the price to be paid for such materials shall be the contractor's established catalog or market price, adjusted to reflect the--

(1) Quantities being acquired; and

(2) Any modifications necessary because of contract requirements.

(B) Except as provided for in paragraph (i)(1)(ii)(A) and (D)(2) of this clause, the Government will reimburse the Contractor the actual cost of materials (less any rebates, refunds, or discounts received by the contractor that are identifiable to the contract) provided the Contractor--

(1) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or

(2) Makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.

(C) To the extent able, the Contractor shall--

(1) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and

(2) Give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that are identifiable to the contract.

(D) Other Costs. Unless listed below, other direct and indirect costs will not be reimbursed.

(1) Other Direct Costs. The Government will reimburse the Contractor on the basis of actual cost for the following, provided such costs comply with the requirements in paragraph (i)(1)(ii)(B) of this clause:

(2) Indirect Costs (Material Handling, Subcontract Administration, etc.). The Government will reimburse the Contractor for indirect costs on a pro-rata basis over the period of contract performance at the following fixed price:

(2) Total cost. It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during the performance of this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performance of this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(3) Ceiling price. The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(4) Access to records. At any time before final payment under this contract, the Contracting Officer (or authorized representative) will have access to the following (access shall be limited to the listing below unless otherwise agreed to by the Contractor and the Contracting Officer):

(i) Records that verify that the employees whose time has been included in any invoice meet the qualifications for the labor categories specified in the contract;

(ii) For labor hours (including any subcontractor hours reimbursed at the hourly rate in the schedule), when timecards are required as substantiation for payment--

(A) The original timecards (paper-based or electronic);

(B) The Contractor's timekeeping procedures;

(C) Contractor records that show the distribution of labor between jobs or contracts; and

(D) Employees whose time has been included in any invoice for the purpose of verifying that these employees have worked the hours shown on the invoices.

(iii) For material and subcontract costs that are reimbursed on the basis of actual cost--

(A) Any invoices or subcontract agreements substantiating material costs; and

(B) Any documents supporting payment of those invoices.

(5) Overpayments/Underpayments. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding invoices, that are found by the Contracting Officer not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. The Contractor shall promptly pay any such reduction within 30 days unless the parties agree otherwise. The Government within 30 days will pay any such increases, unless the parties agree otherwise. The Contractor's payment will be made by check. If the Contractor becomes aware of a duplicate invoice payment or that the Government has otherwise overpaid on an invoice payment, the Contractor shall--

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the--

(A) Circumstances of the overpayment (e.g., duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected contract line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6)(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury, as provided in section 611 of the Contract Disputes Act of 1978 (Public Law 95-563), which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six month period as established by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) Final Decisions. The Contracting Officer will issue a final decision as required by 33.211 if--

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt in a timely manner;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see FAR 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on--

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(viii) Upon receipt and approval of the invoice designated by the Contractor as the "completion invoice" and supporting documentation, and upon compliance by the Contractor with all terms of this contract, any outstanding balances will be paid within 30 days unless the parties agree otherwise. The completion invoice, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(7) Release of claims. The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions.

(i) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible to exact statement by the Contractor.

(ii) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(iii) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(8) Prompt payment. The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(9) Electronic Funds Transfer (EFT). If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(10) Discount. In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(j) Risk of loss. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) Taxes. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) Termination for the Government's convenience. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid an amount for direct labor hours (as defined in the Schedule of the contract) determined by multiplying the number of direct labor hours expended before the effective date of termination by the hourly rate(s) in the contract, less any hourly rate payments already made to the Contractor plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system that have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.

(m) Termination for cause. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) Title. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) Warranty. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) Limitation of liability. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) Other compliances. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) Compliance with laws unique to Government contracts. The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, et seq., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.

(s) Order of precedence. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, and Compliance with Laws Unique to Government Contracts paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any license agreements for computer software.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments

(9) The specification.

(t) Central Contractor Registration (CCR).

(1) Unless exempted by an addendum to this contract, the Contractor is responsible during performance and through final payment of any contract for the accuracy and completeness of the data within the CCR database, and for any liability resulting from the Government's reliance on inaccurate or incomplete data. To remain registered in the CCR database after the initial registration, the Contractor is required to review and update on an annual basis from the date of initial registration or subsequent updates its information in the CCR database to ensure it is current, accurate and complete. Updating information in the CCR does not alter the terms and conditions of this contract and is not a substitute for a properly executed contractual document.

(2)(i) If a Contractor has legally changed its business name, "doing business as" name, or division name (whichever is shown on the contract), or has transferred the assets used in performing the contract, but has not completed the necessary requirements regarding novation and change-of-name agreements in FAR subpart 42.12, the Contractor shall provide the responsible Contracting Officer a minimum of one business day's written notification of its intention to (A) change the name in the CCR database; (B) comply with the requirements of subpart 42.12; and (C)

agree in writing to the timeline and procedures specified by the responsible Contracting Officer. The Contractor must provide with the notification sufficient documentation to support the legally changed name.

(ii) If the Contractor fails to comply with the requirements of paragraph (t)(2)(i) of this clause, or fails to perform the agreement at paragraph (t)(2)(i)(C) of this clause, and, in the absence of a properly executed novation or change-of-name agreement, the CCR information that shows the Contractor to be other than the Contractor indicated in the contract will be considered to be incorrect information within the meaning of the "Suspension of Payment" paragraph of the electronic funds transfer (EFT) clause of this contract.

(3) The Contractor shall not change the name or address for EFT payments or manual payments, as appropriate, in the CCR record to reflect an assignee for the purpose of assignment of claims (see Subpart 32.8, Assignment of Claims). Assignees shall be separately registered in the CCR database. Information provided to the Contractor's CCR record that indicates payments, including those made by EFT, to an ultimate recipient other than that Contractor will be considered to be incorrect information within the meaning of the "Suspension of payment" paragraph of the EFT clause of this contract.

(4) Offerors and Contractors may obtain information on registration and annual confirmation requirements via CCR accessed through https://www.acquisition.gov or by calling 1-888-227-2423 or 269-961-5757.

C.3 2052.215-77 TRAVEL APPROVALS AND REIMBURSEMENT (OCT 1999)

(a) All foreign travel must be approved in advance by the NRC on NRC Form 445, Request for Approval of Official Foreign Travel, and must be in compliance with FAR 52.247-63 Preference for U.S. Flag Air Carriers. The contractor shall submit NRC Form 445 to the NRC no later than 30 days before beginning travel.

(b) The contractor must receive written approval from the NRC Contracting Officer's Representative (COR) before taking travel that 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).

(c) The contractor will be reimbursed only for those travel costs incurred that are directly related to this contract and are allowable subject to the limitations prescribed in FAR 31.205-46.

(d) It is the responsibility of the contractor to notify the contracting officer in accordance with the Limitations of Cost clause of this contract when, at any time, the contractor learns that travel expenses will cause the contractor to exceed the estimated costs specified in the Schedule.

(e) Reasonable travel costs for research and related activities performed at State and nonprofit institutions, in accordance with Section 12 of Pub. L. 100-679, shall be charged in accordance with the contractor's institutional policy to the degree that the limitations of Office of Management and Budget (OMB) guidance are not exceeded. Applicable guidance documents include OMB Circular A-87, Cost Principles for State and Local Governments; OMB Circular A-122, Cost Principles for Nonprofit Organizations; and OMB Circular A-21, Cost Principles for Educational Institutions.

C.4 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days.

C.5 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 eight years and three months.

C.6 52.219-14 LIMITATIONS ON SUBCONTRACTING (NOV 2011)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) Applicability. This clause applies only to-

(1) Contracts that have been set aside or reserved for small business concerns or 8(a) concerns;

(2) Part or parts of a multiple-award contract that have been set aside for small business concerns or 8(a) concerns; and

(3) Orders set aside for small business or 8(a) concerns under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(c) By submission of an offer and execution of a contract, the Offeror/Contractor agrees that in performance of the contract in the case of a contract for--

(1) Services (except construction). At least 50 percent of the cost of contract performance incurred for personnel shall be expended for employees of the concern.

(2) Supplies (other than procurement from a nonmanufacturer of such supplies). The concern shall perform work for at least 50 percent of the cost of manufacturing the supplies, not including the cost of materials.

(3) General construction. The concern will perform at least 15 percent of the cost of the contract, not including the cost of materials, with its own employees.

(4) Construction by special trade contractors. The concern will perform at least 25 percent of the cost of the contract, not including the cost of materials, with its own employees.

C.7 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 requirements; 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.

C.8 52.237-2 PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION (APR 1984)

The Contractor shall use reasonable care to avoid damaging existing buildings, equipment, and vegetation on the Government installation. If the Contractor's failure to use reasonable care causes damage to any of this property, the Contractor shall replace or repair the damage at no expense to the Government as the Contracting Officer directs. If the Contractor fails or refuses to make such repair or replacement, the Contractor shall be liable for the cost, which may be deducted from the contract price.

C.9 52.244-2 SUBCONTRACTS (OCT 2010)

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

"Approved purchasing system" means a Contractor's purchasing system that has been reviewed and approved in accordance with Part 44 of the Federal Acquisition Regulation (FAR).

"Consent to subcontract" means the Contracting Officer's written consent for the Contractor to enter into a particular subcontract.

"Subcontract" means any contract, as defined in FAR Subpart 2.1, entered into by a subcontractor to furnish supplies or services for performance of the prime contract or a subcontract. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.

(b) When this clause is included in a fixed-price type contract, consent to subcontract is required only on unpriced contract actions (including unpriced modifications or unpriced delivery orders), and only if required in accordance with paragraph (c) or (d) of this clause.

(c) If the Contractor does not have an approved purchasing system, consent to subcontract is required for any subcontract that--

(1) Is of the cost-reimbursement, time-and-materials, or labor- hour type; or

(2) Is fixed-price and exceeds--

(i) For a contract awarded by the Department of Defense, the Coast Guard, or the National Aeronautics and Space Administration, the greater of the simplified acquisition threshold or 5 percent of the total estimated cost of the contract; or

(ii) For a contract awarded by a civilian agency other than the Coast Guard and the National Aeronautics and Space Administration, either the simplified acquisition threshold or 5 percent of the total estimated cost of the contract.

(d) If the Contractor has an approved purchasing system, the Contractor nevertheless shall obtain the Contracting Officer's written consent before placing the following subcontracts: None

(e)(1) The Contractor shall notify the Contracting Officer reasonably in advance of placing any subcontract or modification thereof for which consent is required under paragraph (b), (c), or (d) of this clause, including the following information:

(i) A description of the supplies or services to be subcontracted.

(ii) Identification of the type of subcontract to be used.

(iii) Identification of the proposed subcontractor.

(iv) The proposed subcontract price.

(v) The subcontractor's current, complete, and accurate certified cost or pricing data and Certificate of Current Cost or Pricing Data, if required by other contract provisions.

(vi) The subcontractor's Disclosure Statement or Certificate relating to Cost Accounting Standards when such data are required by other provisions of this contract.

(vii) A negotiation memorandum reflecting--

(A) The principal elements of the subcontract price negotiations;

(B) The most significant considerations controlling establishment of initial or revised prices;

(C) The reason certified cost or pricing data were or were not required;

(D) The extent, if any, to which the Contractor did not rely on the subcontractor's certified cost or pricing data in determining the price objective and in negotiating the final price;

(E) The extent to which it was recognized in the negotiation that the subcontractor's certified cost or pricing data were not accurate, complete, or current; the action taken by the Contractor and the subcontractor; and the effect of any such defective data on the total price negotiated;

(F) The reasons for any significant difference between the Contractor's price objective and the price negotiated; and

(G) A complete explanation of the incentive fee or profit plan when incentives are used. The explanation shall identify each critical performance element, management decisions used to quantify each incentive element, reasons for the incentives, and a summary of all trade-off possibilities considered.

(2) The Contractor is not required to notify the Contracting Officer in advance of entering into any subcontract for which consent is not required under paragraph (b), (c), or (d) of this clause.

(f) Unless the consent or approval specifically provides otherwise, neither consent by the Contracting Officer to any subcontract nor approval of the Contractor's purchasing system shall constitute a determination--

(1) Of the acceptability of any subcontract terms or conditions;

(2) Of the allowability of any cost under this contract; or

(3) To relieve the Contractor of any responsibility for performing this contract.

(g) No subcontract or modification thereof placed under this contract shall provide for payment on a cost-plus-a-percentage-of- cost basis, and any fee payable under cost-reimbursement type subcontracts shall not exceed the fee limitations in FAR 15.404- 4(c)(4)(i).

(h) The Contractor shall give the Contracting Officer immediate written notice of any action or suit filed and prompt notice of any claim made against the Contractor by any subcontractor or vendor that, in the opinion of the Contractor, may result in litigation related in any way to this contract, with respect to which the Contractor may be entitled to reimbursement from the Government.

(i) The Government reserves the right to review the Contractor's purchasing system as set forth in FAR Subpart 44.3.

(j) Paragraphs (c) and (e) of this clause do not apply to the following subcontracts, which were evaluated during negotiations: All

C.10 52.244-5 COMPETITION IN SUBCONTRACTING (DEC 1996)

(a) The Contractor shall select subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the contract.

(b) If the Contractor is an approved mentor under the Department of Defense Pilot Mentor-Protégé Program (Pub. L. 101-510, section 831 as amended), the Contractor may award subcontracts under this contract on a noncompetitive basis to its protégés.

C.11 SEAT BELTS

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

C.12 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (APR 2012)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104 (g)).

(2) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Pub. L. 108-77, 108-78)

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[X] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

[X] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010)(Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

[] (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[X] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (FEB 2012) (Pub. L. 109-282) (31 U.S.C. 6101 note).

[] (5) 52.204-11, American Recovery and Reinvestment Act-Reporting Requirements (JUL 2010) (Pub. L. 111-5).

[X] (6) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Dec 2010) (31 U.S.C. 6101 note).

[X] (7) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (JAN 2012) (41 U.S.C. 2313).

[X] (8) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (section 740 of Division C of Public Law 111-117, section 743 of Division D of Public Law 111-8, and section 745 of Division D of Public Law 110-161)

[] (9) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (NOV 2011) (15 U.S.C. 657a).

[] (10) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JAN 2011) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[] (11) [Reserved]

[X] (12)(i) 52.219-6, Notice of Total Small Business Set-Aside (NOV 2011) (15 U.S.C. 644).

[] (ii) Alternate I (NOV 2011).

[] (iii) Alternate II (NOV 2011).

[] (13)(i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

[] (ii) Alternate I (Oct 1995) of 52.219-7.

[] (iii) Alternate II (Mar 2004) of 52.219-7.

[X] (14) 52.219-8, Utilization of Small Business Concerns (JAN 2011) (15 U.S.C. 637(d)(2) and (3)).

[] (15)(i) 52.219-9, Small Business Subcontracting Plan (JAN 2011) (15 U.S.C. 637(d)(4)).

[] (ii) Alternate I (Oct 2001) of 52.219-9.

[] (iii) Alternate II (Oct 2001) of 52.219-9.

[] (iv) Alternate III (JUL 2010) of 52.219-9.

[] (16) 52.219-13, Notice of Set-Aside of Orders (NOV 2011) (15 U.S.C. 644(r)).

[X] (17) 52.219-14, Limitations on Subcontracting (NOV 2011) (15 U.S.C. 637(a)(14)).

[] (18) 52.219-16, Liquidated Damages--Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[] (19)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (OCT 2008) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer.)

[] (ii) Alternate I (June 2003) of 52.219-23.

[] (20) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (DEC 2010) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (21) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (Oct 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

[] (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (NOV 2011) (15 U.S.C. 657f).

[X] (23) 52.219-28, Post Award Small Business Program Rerepresentation (APR 2009) (15 U.S.C 632(a)(2)).

[] (24) 52.219-29, Notice of Set-Aside for Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (APR 2012) (15 U.S.C. 637(m)).

[] (25) 52.219-30, Notice of Set-Aside for Women-Owned Small Business (WOSB) Concerns Eligible Under the WOSB Program (APR 2012) (15 U.S.C. 637(m)).

[X] (26) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

[X] (27) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (MAR 2012) (E.O. 13126).

[X] (28) 52.222-21, Prohibition of Segregated Facilities (Feb 1999).

[X] (29) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

[X] (30) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

[X] (31) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

[X] (32) 52.222-37, Employment Reports on Veterans (SEP 2010) (38 U.S.C. 4212).

[] (33) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

[X] (34) 52.222-54, Employment Eligibility Verification (Jan 2009). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[] (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C.6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[] (36) 52.223-15, Energy Efficiency in Energy-Consuming Products (DEC 2007)(42 U.S.C. 8259b).

[] (37)(i) 52.223-16, IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007) (E.O. 13423).

[] (ii) Alternate I (DEC 2007) of 52.223-16.

[X] (38) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (AUG 2011)

[] (39) 52.225-1, Buy American Act--Supplies (FEB 2009) (41 U.S.C. 10a-10d).

[] (40)(i) 52.225-3, Buy American Act--Free Trade Agreements-- Israeli Trade Act (MAR 2012) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, Pub. L. 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, and Pub. L. 112-41).

[] (ii) Alternate I (MAR 2012) of 52.225-3.

[] (iii) Alternate II (MAR 2012) of 52.225-3.

[] (iv) Alternate III (MAR 2012) of 52.225-3.

[] (41) 52.225-5, Trade Agreements (MAR 2012) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

[X] (42) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[] (43) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

[] (44) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

[] (45) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[] (46) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

[X] (47) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (Oct 2003) (31 U.S.C. 3332).

[] (48) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (May 1999) (31 U.S.C. 3332).

[] (49) 52.232-36, Payment by Third Party (FEB 2010) (31 U.S.C. 3332).

[] (50) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

[] (51)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

[] (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[] (1) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

[] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

Employee Class Monetary Wage-Fringe Benefits

[] (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Sep 2009) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

[] (5) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

[] (6) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

[] (7) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247)

[] (8) 52.237-11, Accepting and Dispensing of $1 Coin (SEP 2008) (31 U.S.C. 5112(p)(1)).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records--Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note)).

(ii) 52.219-8, Utilization of Small Business Concerns (DEC 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) [Reserved]

(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Veterans (SEP 2010) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).

(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements "(Nov 2007)" (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (FEB 2009)(41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employee Eligibility Verification (JAN 2009)

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009)(Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

C.13 2052.204.70 SECURITY (MAR 2004)

(a) Contract Security and/or Classification Requirements (NRC Form 187). The policies, procedures, and criteria of the NRC Security Program, NRC Management Directive (MD) 12 (including MD 12.1, "NRC Facility Security Program;" MD 12.2, "NRC Classified Information Security Program;" MD 12.3, "NRC Personnel Security Program;" MD 12.4, "NRC Telecommunications Systems Security Program;" MD 12.5, "NRC Automated Information Systems Security Program;" and MD 12.6, "NRC Sensitive Unclassified Information Security Program"), apply to performance of this contract, subcontract or other activity. This MD is incorporated into this contract by reference as though fully set forth herein. The attached NRC Form 187 (See List of Attachments) furnishes the basis for providing security and classification requirements to prime contractors, subcontractors, or others (e.g., bidders) who have or may have an NRC contractual relationship that requires access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (e.g., Safeguards), access to sensitive Information Technology (IT) systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants.

(b) It is the contractor's duty to protect National Security Information, Restricted Data, and Formerly Restricted Data. The contractor shall, in accordance with the Commission's security regulations and requirements, be responsible for protecting National Security Information, Restricted Data, and Formerly Restricted Data, and for protecting against sabotage, espionage, loss, and theft, the classified documents and material in the contractor's possession in connection with the performance of work under this contract. Except as otherwise expressly provided in this contract, the contractor shall, upon completion or termination of this contract, transmit to the Commission any classified matter in the possession of the contractor or any person under the contractor's control in connection with performance of this contract. If retention by the contractor of any classified matter is required after the completion or termination of the contract and the retention is approved by the contracting officer, the contractor shall complete a certificate of possession to be furnished to the Commission specifying the classified matter to be retained. The certification must identify the items and types or categories of matter retained, the conditions governing the retention of the matter and

their period of retention, if known. If the retention is approved by the contracting officer, the security provisions of the contract continue to be applicable to the matter retained.

(c) In connection with the performance of the work under this contract, the contractor may be furnished, or may develop or acquire, safeguards information, or confidential or privileged technical, business, or financial information, including Commission plans, policies, reports, financial plans, internal data protected by the Privacy Act of 1974 (Pub. L. 93.579), or other information which has not been released to the public or has been determined by the Commission to be otherwise exempt from disclosure to the public. The contractor shall ensure that information protected from public disclosure is maintained as required by NRC regulations and policies, as cited in this contract or as otherwise provided by the NRC. The contractor will not directly or indirectly duplicate, disseminate, or disclose the information in whole or in part to any other person or organization except as may be necessary to perform the work under this contract. The contractor agrees to return the information to the Commission or otherwise dispose of it at the direction of the contracting officer. Failure to comply with this clause is grounds for termination of this contract.

(d) Regulations. The contractor agrees to conform to all security regulations and requirements of the Commission which are subject to change as directed by the NRC Division of Facilities and Security (DFS) and the Contracting Officer. These changes will be under the authority of the FAR Changes clause referenced in this document.

The contractor agrees to comply with the security requirements set forth in NRC Management Directive 12.1, NRC Facility Security Program which is incorporated into this contract by reference as though fully set forth herein. Attention is directed specifically to the section titled "Infractions and Violations," including "Administrative Actions" and "Reporting Infractions."

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

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

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

(h) Definition of Safeguards Information. Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant for the physical protection of special nuclear material; or security measures for the physical protection and location of certain plant equipment vital to the safety of production of utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

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

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

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

(l) In performing the contract work, the contractor shall classify all documents, material, and equipment originated or generated by the contractor in accordance with guidance issued by the Commission. Every subcontract and purchase order issued hereunder involving the origination or generation of classified documents, material, and equipment must provide that the subcontractor or supplier assign classification to all documents, material, and equipment in accordance with guidance furnished by the contractor.

C.14 2052.204-71 BADGE REQUIREMENTS FOR UNESCORTED BUILDING ACCESS TO NRC FACILITIES (MAR 2006)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available, as required, provided that the individual has been approved for unescorted access after a favorable adjudication from the Security Branch, Division of Facilities and Security (SB/DFS).

In this regard, all contractor personnel whose duties under this contract require their presence on site shall be clearly identifiable by a distinctive badge furnished by the NRC. The COR shall assist the contractor in obtaining badges for the contractor personnel. All contractor personnel must present two forms of Identity Source Documents (I-9). One of the documents must be a valid picture ID issued by a state or by the Federal Government. Original I-9 documents must be presented in person for certification. A list of acceptable documents can be found at http://www.usdoj.gov/crt/recruit_employ/i9form.pdf. It is the sole responsibility of the contractor to ensure that each employee has a proper NRC-issued identification/badge at all times. All photo-identification badges must be immediately (no later than three days) delivered to SB/DFS for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel must display any NRC issued badge in clear view at all times during on site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work, and to assure the protection of any Government records or data that contractor personnel may come into contact with.

C.15 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY LEVEL I OR LEVEL II ACCESS APPROVAL (AUG 2011)

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

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

(a) felony arrest in the last seven (7) years; (b) alcohol related arrest within the last five (5) years; (c) record of any military courts-martial convictions in the past ten (10) years; (d) illegal use of narcotics or other controlled substances possession in the past year, or illegal purchase, production, transfer, or distribution of narcotics or other controlled substances in the last seven (7) years; and (e) delinquency on any federal debts or bankruptcy in the last seven (7) years.

The contractor shall make a written record of its pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (e)), and have the employee verify the pre-screening record or review, sign and date it. The contractor shall supply two (2) copies of the signed contractor's pre-screening record or review

to the NRC Contracting Officer's Representative (COR), who will then provide them to the NRC Office of Administration, Division of Facilities and Security, Personnel Security Branch with the employee's completed IT access application package.

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

SECURITY REQUIREMENTS FOR IT LEVEL I

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

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

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

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

have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems and data; access on a continuing basis (in excess more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

SECURITY REQUIREMENTS FOR IT LEVEL II

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

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

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

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

In accordance with NRCAR 2052.204-70 "Security," IT Level II contractors shall be subject to the attached NRC Form 187, SF-86, and contractor's record of the pre-screening which furnishes the basis for providing security requirements to contractors that have or may have an NRC contractual relationship which requires access to or operation of agency sensitive information technology systems or remote development and/or analysis of sensitive information technology systems or data or other access to such systems or data; access on a continuing basis (in excess of more than 30 calendar days) to NRC buildings; or otherwise requires issuance of an unescorted NRC badge.

CANCELLATION OR TERMINATION OF IT ACCESS/REQUEST

When a request for IT access is to be withdrawn or canceled, the contractor shall immediately notify the NRC Contracting Officer's Representative (COR) by telephone so that the access review may be promptly discontinued.

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

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

C.16 RULES OF BEHAVIOR FOR AUTHORIZED COMPUTER USE (MAR 2011)

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 Automated Information 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.

C.17 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 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 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.

C.18 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (AUG 2011)

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.

C.19 2052.215-71 CONTRACTING OFFICER REPRESENTATIVE (NOVEMBER 2006)

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

Name: *

Address: *

Telephone Number: *TO BE SPECIFIED UPON TASK ORDER AWARD

(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 (SOW) or changes to specific travel identified in the SOW), fills in details, or otherwise serves to accomplish the contractual SOW.

(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, approval of 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 as 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 the 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 thereto 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.

(4) Assist the contractor in obtaining the badges for the contractor personnel.

(5) Immediately notify the Security Branch, Division of Facilities and Security (SB/DFS) (via e-mail) when a contractor employee no longer requires access authorization and return of any NRC issued badge to SB/DFS within three days after their termination.

(6) Ensure that all contractor employees that require access to classified Restricted Data or National Security Information or matter, access to sensitive unclassified information (Safeguards, Official Use Only, and Proprietary information) access to sensitive IT systems or data, unescorted access to NRC controlled buildings/space, or unescorted access to protected and vital areas of nuclear power plants receive approval of SB/DFS prior to access in accordance with Management Directive and Handbook 12.3.

(7) For contracts for the design, development, maintenance or operation of Privacy Act Systems of Records, obtain from the contractor as part of closeout procedures, written certification that the contractor has returned to NRC, transferred to the successor contractor, or destroyed at the end of the contract in accordance with instructions provided by the NRC Systems Manager for Privacy Act Systems of Records, all records (electronic or paper) which were created, compiled, obtained or maintained under the contract.

C.20 BRANDING (AUG 2011)

The Contractor is required to use the official NRC branding logo or seal on any publications, presentations, products, or materials funded under this task order, to the extent practical, in order to provide NRC 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.

Access the following websites for branding information and specifications:
http://www.internal.nrc.gov/ADM/branding/ and Management Directive and Handbook 3.13 -

(internal NRC website): http://www.internal.nrc.gov/policy/directives/toc/md3.13.htm

(external public website): http://pbadupws.nrc.gov/docs/ML1122/ML112280190.pdf

C.21 PLACE OF DELIVERY--REPORTS (AUG 2011)

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

a. Name: (1 hard copy)
b. Contracting Officer's Representative (COR)
c. U.S. Nuclear Regulatory Commission
d. Address:

U.S. Nuclear Regulatory Commission
Washington, DC
20555

e. Electronic copies to:
f. (List names and email addresses)

C.22 PERIOD OF PERFORMANCE (AUG 2011) ALTERNATE II (AUG 2011)

This contract shall commence on August 31, 2012 and will expire on August 30, 2013.

Base Period:	August 31, 2012 - August 30, 2013
Option Period 1:	August 31, 2013 - August 30, 2014
Option Period 2:	August 31, 2014 - August 30, 2015
Option Period 3:	August 31, 2015 - August 30, 2016
Option Period 4:	August 31, 2016 - August 30, 2017
Option Period 5:	August 31, 2017 - August 30, 2018
Option Period 6:	August 31, 2018 - August 30, 2019
Option Period 7:	August 31, 2019 - August 30, 2020
Option Period 8:	August 31, 2020 - November 30, 2020

C.23 ELECTRONIC PAYMENT (AUG 2011)

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

To receive payment, the contractor shall prepare invoices in accordance with NRC's Billing Instructions. Claims shall be submitted on the payee's letterhead, invoice, or on the Government's Standard Form 1034, "Public Voucher for Purchases and Services Other than Personal," and Standard Form 1035, "Public Voucher for Purchases Other than Personal - Continuation Sheet." The preferred method of submitting invoices is electronically to the Department of the Interior at NRCPayments_NBCDenver@nbc.gov. If the contractor submits a hard copy of the invoice, it shall be submitted to the following address:

Department of the Interior
National Business Center
Attn: Fiscal Services Branch - D2770
7301 West Mansfield Avenue
Denver, CO 80235-2230

C.24 DENIAL OF FEDERAL BENEFITS TO INDIVIDUALS CONVICTED OF DRUG TRAFFICKING OR POSSESSION (AUG 2011)

In the event that an award is made to an individual, Section 5301 of the Anti-Drug Abuse Act of 1988 (P.L. 100-690), codified at 21 U.S.C. 862, authorizes denial of Federal benefits such as grants, contracts, purchase orders, financial aid, and business and professional licenses to individuals convicted of drug trafficking or possession.

C.25 COMPENSATION FOR ON-SITE CONTRACTOR PERSONNEL (AUG 2011) ALTERNATE I (AUG 2011)

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

(b) When NRC facilities are unavailable, the compensation and deduction policy stated below shall be followed for contractor employees performing work on-site at the NRC facility:

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

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

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

*To be incorporated into the resultant contract

C.26 COMPLIANCE WITH U.S. IMMIGRATION LAWS AND REGULATIONS (AUG 2011)

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

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

C.27 SECURITY REQUIREMENTS RELATING TO THE PRODUCTION OF REPORT(S) OR THE PUBLICATION OF RESULTS UNDER CONTRACTS, AGREEMENTS, AND GRANTS (AUG 2011)

Review and Approval of Reports

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

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

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

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

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

C.28 WHISTLEBLOWER PROTECTION FOR NRC CONTRACTOR AND SUBCONTRACTOR EMPLOYEES (AUG 2011)

(a) The U.S. Nuclear Regulatory Commission (NRC) contractor and its subcontractor are subject to the Whistleblower Employee Protection public law provisions as codified at 42 U.S.C. 5851. NRC contractor(s) and subcontractor(s) shall comply with the requirements of this Whistleblower Employee Protection law, and the implementing regulations of the NRC and the Department of Labor (DOL). See, for example, DOL Procedures on Handling Complaints at 29 C.F.R. Part 24 concerning the employer obligations, prohibited acts, DOL procedures and the requirement for prominent posting of notice of Employee Rights at Appendix A to Part 24 entitled: "Your Rights Under the Energy Reorganization Act".

(b) Under this Whistleblower Employee Protection law, as implemented by regulations, NRC contractor and subcontractor employees are protected from discharge, reprisal, threats, intimidation, coercion, blacklisting or other employment discrimination practices with respect to compensation, terms, conditions or privileges of their employment because the contractor or subcontractor employee(s) has provided notice to the employer, refused to engage in unlawful practices, assisted in proceedings or testified on activities concerning alleged violations of the Atomic Energy Act of 1954 (as amended) and the Energy Reorganization Act of 1974 (as amended).

(c) The contractor shall insert this or the substance of this clause in any subcontracts involving work performed under this contract.

C.29 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (AUG 2011)

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

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

(2) Removal from the space occupied

(3) Contract Termination

C.30 GREEN PURCHASING (JUN 2011)

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

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

C.31 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS (AUG 2011)

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

C.32 PERSONNEL REQUIREMENTS

This task order requires work with classified and unclassified information and systems. Some Contractor personnel may require an "L" or a "Q" clearance. All Contractor personnel with access to NRC information systems or NRC sensitive information must have an IT Level I or II approved access in accordance with Management Directive 12.3, NRC Personnel Security Program.

C.33 RIGHTS IN DATA – SPECIAL WORKS (DEC 2007)

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

"Data" means recorded information, regardless of form or the medium 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 for copyright.

(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 which 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 subparagraph (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 D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

ATTACHMENT	TITLE
A	STATEMENT OF WORK
B	BILLING INSTRUCTIONS TIME AND MATERIALS
C	BILLING INSTRUCTIONS FIXED PRICE
D	COST/PRICE SCHEDULE
E	LIST OF CONTRACTS FORM
F	PAST PERFORMANCE QUESTIONNAIRE
G	NRC 187 (PROVIDED UPON AWARD)
H	OCOI GUIDELINES
I	MONTHLY PROGRESS REPORT FORMAT

SECTION E - SOLICITATION PROVISIONS

E.1 2052.209-71 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST (REPRESENTATION) (OCT 1999)

I represent to the best of my knowledge and belief that:

The award to _____of a contract or the modification of an existing contract does / / does not / / involve situations or relationships of the type set forth in 48 CFR 2009.570-3(b).

(a) If the representation, as completed, indicates that situations or relationships of the type set forth in 48 CFR 2009.570-3(b) are involved, or the contracting officer otherwise determines that potential organizational conflicts of interest exist, the Offeror shall provide a statement in writing which describes in a concise manner all relevant factors bearing on his representation to the contracting officer. If the contracting officer determines that organizational conflicts exist, the following actions may be taken:

(1) Impose appropriate conditions which avoid such conflicts,

(2) Disqualify the Offeror, or

(3) Determine that it is otherwise in the best interest of the United States to seek award of the contract under the waiver provisions of 48 CFR 2009-570-9.

(b) The refusal to provide the representation required by 48 CFR 2009.570-4(b), or upon request of the contracting officer, the facts required by 48 CFR 2009.570-3(b), must result in disqualification of the Offeror for award.

E.2 ADDENDUM to FAR 52.212-1 Instructions to Offerors-- Commercial Items

Provisions that are incorporated by reference (by Citation Number, Title, and Date), have the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The following provisions are incorporated as an addendum to this solicitation:

E.3 52.216-31 TIME-AND-MATERIALS/LABOR-HOUR PROPOSAL REQUIREMENTS-- COMMERCIAL ITEM ACQUISITION (FEB 2007)

(Applies to all T&M CLINs in Section B.1.)

(a) The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.

(b) The Offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The Offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by--

(1) The Offeror;

(2) Subcontractors; and/or

(3) Divisions, subsidiaries, or affiliates of the Offeror under a common control.

E.4 2052.209-70 CURRENT/FORMER AGENCY EMPLOYEE INVOLVEMENT (OCT 1999)

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

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

E.5 52.233-2 SERVICE OF PROTEST (SEP 2006)

(a) Protests, as defined in Section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from: Joseph Widdup.

Hand-Carried Address:

U.S. Nuclear Regulatory Commission
Division of Contracts
Attn: Joseph L. Widdup, Contracting Officer
12300 Twinbrook Parkway
Rockville, MD 20852
M/F: Solicitation No. NRC-HQ-12-4-33-0067

Mailing Address:

U.S. Nuclear Regulatory Commission
Div. of Contracts
Attn: Joseph L. Widdup, Contracting Officer

Mail Stop: TWB-01-B10M
Washington, DC 20555-0001
M/F: Solicitation No. NRC-HQ-12-4-33-0067
Email Address: joseph.widdup@nrc.gov

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

E.6 2052.215-73 AWARD NOTIFICATION AND COMMITMENT OF PUBLIC FUNDS (OCT 1999)

(a) All Offerors will be notified of their exclusion from the competitive range in accordance with FAR 15.503(a)(1). Under the requirements of FAR 15.503(a)(2), preliminary notification will be provided before award for small business set-aside procurements on negotiated procurements. The contracting officer shall provide written post-award notice to each unsuccessful Offeror in accordance with FAR 15.503(b).

(b) The contracting officer is the only individual who can legally 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 informal contractual commitments, or otherwise bind, commit, or obligate the NRC contractually. Informal contractual commitments include:

(1) Encouraging a potential Contractor to incur costs before 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.

E.7 2052.215-74 DISPOSITION OF PROPOSALS (JAN 1993)

After award of the contract, one copy of each unsuccessful proposal is retained by the NRC's Division of Contracts in accordance with the General Records Schedule 3(5)(b). Unless return of the additional copies of the proposals is requested by the Offeror upon submission of the proposals, all other copies will be destroyed. This request should appear in a cover letter accompanying the proposal.

E.8 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 requirements; 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.

E.9 ADDENDUM TO PROVISION 52.212-1

ADDENDUM TO PROVISION 52.212-1; PROPOSAL SUBMISSION INSTRUCTIONS

The following paragraphs replace paragraphs (b) and (c) in provision 52.212-1:

(b) *Submission of offers*. Submit signed and dated GSA Alliant Small Business GWAC offers VIA GSA E-BUY ONLY at or before the exact time specified in this solicitation. Offers may be submitted on the SF 1449, letterhead stationery, or as otherwise specified in the solicitation. Only GSA Alliant Small Business GWAC offers will be considered.As a minimum, offers must show—

(1) The solicitation number;

(2) The name, address, telephone number and email address of the offeror;

(3) A description of how the offeror intends to comply with the requirements of clauses 52.219-6, 52.219-14 and 52.244-2;

(4) A detailed submission for technical approach and personnel qualifications (see below);

(5) Proposed cost/price for the base period and each option year, including and any discount terms (see below);

(6) Acknowledgment of Solicitation Amendments;

(7) Indication of whether the Offeror has an approved purchasing system as defined in FAR Part 44 and, if so, a copy of the written approval from the Government for the Offeror's purchasing system.

(8) A copy of provisions E.1 and E.4 from this solicitation, completed by the Offeror;

(9) Past performance information, to include recent and relevant contracts for the same or similar items and other references (including contract numbers, points of contact with telephone numbers and other relevant information) (see below); and

(10) If the offer is not submitted on the SF 1449, include a statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation. Offers that fail to furnish required representations or information, or reject the terms and conditions of the solicitation may be excluded from consideration.

(c) Period for acceptance of offers. The offeror agrees to hold the prices in its offer firm for at least 120 calendar days from the date specified for receipt of offers.

Information submitted in response to this solicitation must be typed, printed, or reproduced on letter-size paper and each copy must be legible. All text information should be printed in Arial 11 point font. Tables, charts, diagrams, and illustrations may be up to 11" x 17" foldouts, as appropriate for the subject matter, and must be folded to 8 1/2" x 11" size. The length of the total Technical Quote submission is limited to **75 single-sided pages**. The following items are excluded from the 75 page limitation; however, some of these items have individual page limitations: quotation cover letter, title page, table of contents, dividers, acronym lists, organization charts, glossary, personnel resumes (not to exceed 5 pages each), appendices, and past performance information references (not to exceed 1 page each). Foldouts are considered part of the page limitation. Any pages beyond the 75 page limitation will not be evaluated.

The proposal shall contain a statement indicating the period of time the proposal is in effect (not less than 120 days).

ORGANIZATION OF THE PROPOSAL

Part 1 - Non-Cost/Price Portion of the Proposal

(1) This section of the proposal may not contain any reference to cost/price. Resource information, such as data concerning labor hours and categories, materials, subcontracts, travel, computer time, etc., must be included so that the Offeror's understanding of the In scope of work may be evaluated.

(2) The Offeror shall submit in information as set forth below to permit the Government to make a thorough evaluation and sound determination that the proposed approach will have a reasonable likelihood of meeting the requirements and objectives of this procurement.

(3) This portion of the proposal should be tailored to assure that all information reflects a one-to-one relationship to the evaluation criteria.

(4) Statements which paraphrase the Statement of Work without communicating the specific approach proposed by the Offeror, or statements to the effect that the Offeror's understanding can or will comply, with the Statement of Work may be construed as an indication of the Offeror's lack of understanding of the Statement of Work and objectives.

(5) This section of the proposal shall contain excerpts from the Offeror's GSA Alliant Small Business GWAC with the list of labor categories, descriptions of duties/functions of those labor categories, and, if applicable, minimum qualifications for those labor categories.

Part 2 – Administrative Information and Cost/Price Portion of the Proposal

This portion of the proposal shall be submitted separately from the remainder of the proposal.

This portion of the proposal shall contain:

Acknowledgment of Solicitation Amendments;

Indication of whether the Offeror has an approved purchasing system as defined in FAR Part 44 and, if so, a copy of the written approval from the Government for the Offeror's purchasing system.

A copy of provisions E.1 and E.4 from this solicitation, completed by the Offeror;

A worksheet that is readable in Microsoft Excel which includes pertinent details sufficient to show the elements of cost/price upon which the total cost is predicated. The cost/price portion of the proposal shall I include pricing for all personnel, materials, hardware, software, supplies, equipment, travel, and other direct costs necessary to accomplish the performance of the tasks described in the SOW. The cost/price portion of the proposal shall provide a breakdown by GSA Alliant Small Business GWAC contract labor category, estimated labor hours for each labor category, GSA Alliant Small Business GWAC contract fixed hourly rates, discounted as appropriate; and a total amount for each task, including the optional tasks. The cost/price proposal shall include a complete copy of the Offeror's GSA Alliant Small Business GWAC contract, including terms and conditions, labor categories, fixed hourly rates and any contract modifications.

CONTENTS OF NON-COST/PRICE PORTION OF THE PROPOSAL

1. **TECHNICAL APPROACH**

   A. The Offeror shall demonstrate its understanding of the tasks to be performed under this task order, and its proposed approach to satisfy SOW requirements, as well.

   B. The Offeror shall indicate how it intends to satisfy the requirements of FAR clauses 52.219-6, 52.219-14 and 52.244-2 in performing this task order.

2. **PERSONNEL QUALIFICATIONS**

For each person proposed as Key Personnel under this task order, the Offeror shall provide a resume not to exceed five pages in length. The resume shall include their name, their proposed GSA Alliant Small Business GWAC labor category, their education, their experience, any applicable professional certifications, their current country of citizenship and the company name of their current employer (if applicable). The resume shall reflect the individual's experience, education, certifications and other training or certifications associated with the specific needs of performing the effort described in the statement of work, and should not be general in nature. The resume shall also indicate the person's current country of citizenship. Also, the resume should demonstrate which labor category the resume corresponds to from the Offeror's GSA Alliant Small Business GWAC CONTRACT and how it at least meets all functional, performance, education and/or experience criteria for the applicable proposed labor category from that Offeror's GSA Alliant Small Business GWAC contract.

3. **CORPORATE EXPERIENCE**

The Offeror shall complete Attachment E and list relevant experience .

Discuss your organization's relevant experience and the extent to which the necessary experience is currently available within your organization.

4. **PAST PERFORMANCE INFORMATION**

The Offeror shall complete the enclosed (Attachment F) for contracts completed within the past three (3) years or currently being performed that are similar in scope to this requirement – a minimum of three (3), if possible. The NRC reserves the right to query any databases (Ex. Past Performance Information Retrieval System - PPIRS.gov) that may contain past performance information of Offerors, or to obtain past performance information from any other source, as applicable. The NRC may, but is not required to, contact any and all of the referenced points of contact provided on the list of contracts submitted in factor 3(a) above that are similar in scope to this requirement.

List any awards received, provide letters of commendation, etc., that will demonstrate your organization's record of past performance. Also, list any problems encountered and corrective actions taken relating to contractor performance. Provide any other pertinent information that will aid in the evaluation of your organization's past performance record.

The Offeror shall list and discuss all prior contracts terminated for default or for cause and whether any show cause letters, cure notices, or poor performance letters have been received. If the Offeror has not received any of these types of notices or terminations, then the Offerorshould indicate that none have been received. The Offeror shall submit past performance information references for contracts performed in the past 3 years, or currently being performed, for work with similar scope to this RFP. If the Offeror is proposing subcontractor(s) for a significant or critical portion of this solicitation, then the Offeror must provide references for contracts performed in the past 3 years or currently being performed by the subcontractor. For purposes of this solicitation, critical or significant means any effort for which a single subcontractor is proposed to perform at least 10% of the overall SOW requirements.

E.10 52.212-2 Evaluation—Commercial Items (JAN 1999)

(a) The Government intends to award a single task order to the GSA Alliant Small Business GWAC offeror whose proposal is deemed to represent the best value to the Government, cost/price and other factors considered.

The following criteria will be used to evaluate proposals. Factor 1 is the most important factor and is slightly more important than the other non-cost/price factors, which are all approximately equal in importance. Non-cost/price factors 1 through 4 below, when combined, are approximately equally important to factor 5. The Government may perform cost realism analysis in evaluating factor 5 and may consider any adjustments made through that cost realism analysis for source selection purposes.

1. **TECHNICAL APPROACH**

(a) The Government will evaluate the extent to which the offeror demonstrates an adequate or better understanding of the statement of work as reflected in this requirement and demonstrates a sound technical approach and comprehensive implementation plan, including its approach for achieving the technical objectives, as well as its approach to resolving potential problem areas for the work described in this effort.

(b) The Government will evaluate the extent to which the offeror demonstrates an adequate or better solution for complying with FAR clauses 52.219-6, 52.219-14 and 52.244-2.

2. **PERSONNEL QUALIFICATIONS**

The Government will evaluate (a) the extent to which the proposed resumes of key personnel demonstrate adequate or better qualifications to satisfy the minimum qualifications for the applicable GSA Alliant Small Business GWAC labor categories; and (b) the extent to which the proposed labor category mix could reasonably be expected to adequately address the requirements of the solicitation."

Note, in this RFP, Key Personnel includes supervisory personnel or leaders that will be directly engaged in task order performance and any senior-level subject matter experts that are proposed to be engaged in task order performance.

3. **CORPORATE EXPERIENCE**

The Government will evaluate the extent to which the offeror's proposal demonstrates adequate or better corporate experience that is similar in scope to the solicitation requirements.

4. **PAST PERFORMANCE INFORMATION**

Past performance information is one indicator of an offeror's ability to perform the contract successfully. The currency and relevance of the information, source of the information, context of the data, and general trends in contractor's performance will be considered. The Government will evaluate the offeror's past performance on past or current contracts and/or orders (including Federal, State, local government and private) performed) within the past three (3) years, that are similar in scope to the solicitation requirements. The Government will consider information on problems encountered by the offeror on the identified contracts and the offeror's corrective actions. The Government may also consider letters of commendation from commercial clients and/or Federal Government agencies, certificates of appreciation, or awards received showing a high level of performance and customer satisfaction. The Government may rely on past performance information obtained from sources other than the offeror in evaluating this factor of the offeror's proposal. In the event that the offeror has no record of relevant past performance or for whom information in past performance is not available, the Government would assign a neutral rating for this factor. The evaluation may also take into account past performance information regarding predecessor companies, key personnel who have relevant experience, or subcontractors that are proposed to perform major or critical aspects of the requirement when such information is relevant to the instant acquisition. In this RFP, Key Personnel includes supervisory personnel or leaders that will be directly engaged in task order performance and any senior-level subject matter experts that are proposed to be engaged in task order performance.

5. **COST/PRICE**

The Government will add the total cost of all labor categories for the base period to derive the proposed cost/price, and the Government will add the total proposed cost/price for each option period to the total cost/price for the base period to derive the total proposed cost/price for the proposal. The Government may perform cost realism analysis to derive an evaluated cost/price for each contract year and for the entire proposal. The proposed fixed hourly labor rates shall not exceed the fixed hourly labor rates in the offeror's current GSA Alliant Small Business GWAC contract. The Government strongly encourages proposed discounts to the offeror's current GSA Alliant Small Business GWAC contract fixed hourly rates. For proposal preparation purposes, the offeror should assume a task order award date of August 31, 2012 and the period of performance for the task order to begin on September 28, 2012.

(b) *Options*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

(c) A written notice of award or acceptance of an offer, mailed or otherwise furnished to the successful offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party.

Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

NRCAR Subpart 2009.5 Organizational Conflicts of Interest

§2009.500 Scope of subpart.

In accordance with 42 U.S.C. 2210a., NRC acquisitions are processed in accordance with §2009.570, which takes precedence over FAR 9.5 with respect to organizational conflicts of interest. Where non-conflicting guidance appears in FAR 9.5, that guidance must be followed.

§2009.570 NRC organizational conflicts of interest.

§2009.570-1 Scope of policy.

(a) It is the policy of NRC to avoid, eliminate, or neutralize contractor organizational conflicts of interest. The NRC achieves this objective by requiring all prospective contractors to submit information describing relationships, if any, with organizations or persons (including those regulated by the NRC) which may give rise to actual or potential conflicts of interest in the event of contract award.

(b) Contractor conflict of interest determinations cannot be made automatically or routinely. The application of sound judgment on virtually a case-by-case basis is necessary if the policy is to be applied to satisfy the overall public interest. It is not possible to prescribe in advance a specific method or set of criteria which would serve to identify and resolve all of the contractor conflict of interest situations that might arise. However, examples are provided in these regulations to guide application of this policy guidance. The ultimate test is as follows: Might the contractor, if awarded the contract, be placed in a position where its judgment may be biased, or where it may have an unfair competitive advantage?

(c) The conflict of interest rule contained in this subpart applies to contractors and offerors only. Individuals or firms who have other relationships with the NRC (e.g., parties to a licensing proceeding) are not covered by this regulation. This rule does not apply to the acquisition of consulting services through the personnel appointment process, NRC agreements with other Government agencies, international organizations, or state, local, or foreign Governments. Separate procedures for avoiding conflicts of interest will be employed in these agreements, as appropriate.

§2009.570-2 Definitions.

Affiliates means business concerns which are affiliates of each other when either directly or indirectly one concern or individual controls or has the power to control another, or when a third party controls or has the power to control both.

Contract means any contractual agreement or other arrangement with the NRC except as provided in §2009.570-1(c).

Contractor means any person, firm, unincorporated association, joint venture, co-sponsor, partnership, corporation, affiliates thereof, or their successors in interest, including their chief executives, directors, key personnel (identified in the contract), proposed consultants or subcontractors, which are a party to a contract with the NRC.

Evaluation activities means any effort involving the appraisal of a technology, process, product, or policy.

Offeror or prospective contractor means any person, firm, unincorporated association, joint venture, co-sponsor, partnership, corporation, or their affiliates or successors in interest, including their chief executives, directors, key personnel, proposed consultants, or subcontractors, submitting a bid or proposal, solicited or unsolicited, to the NRC to obtain a contract.

Organizational conflicts of interest means that a relationship exists whereby a contractor or prospective contractor has present or planned interests related to the work to be performed under an NRC contract which:

(1) May diminish its capacity to give impartial, technically sound, objective assistance and advice, or may otherwise result in a biased work product; or

(2) May result in its being given an unfair competitive advantage.

Potential conflict of interest means that a factual situation exists that suggests that an actual conflict of interest may arise from award of a proposed contract. The term potential conflict of interest is used to signify those situations that

(1) Merit investigation before contract award to ascertain whether award would give rise to an actual conflict; or

(2) Must be reported to the contracting officer for investigation if they arise during contract performance.

Research means any scientific or technical work involving theoretical analysis, exploration, or experimentation.

Subcontractor means any subcontractor of any tier who performs work under a contract with the NRC except subcontracts for supplies and subcontracts in amounts not exceeding $10,000.

Technical consulting and management support services means internal assistance to a component of the NRC in the formulation or administration of its programs, projects, or policies which normally require that the contractor be given access to proprietary information or to information that has not been made available to the public. These services typically include assistance in the preparation of program plans, preliminary designs, specifications, or statements of work.

§2009.570-3 Criteria for recognizing contractor organizational conflicts of interest.

(a) General.

(1) Two questions will be asked in determining whether actual or potential organizational conflicts of interest exist:

(i) Are there conflicting roles which might bias an offeror's or contractor's judgment in relation to its work for the NRC?

(ii) May the offeror or contractor be given an unfair competitive advantage based on the performance of the contract?

(2) NRC's ultimate determination that organizational conflicts of interest exist will be made in light of common sense and good business judgment based upon the relevant facts. While it is difficult to identify and to prescribe in advance a specific method for avoiding all of the various situations or relationships that might involve potential organizational conflicts of interest, NRC personnel will pay particular attention to proposed contractual requirements that call for the rendering of advice, consultation or evaluation activities, or similar activities that directly lay the groundwork for the NRC's decisions on regulatory activities, future procurements, and research programs. Any work performed at an applicant or licensee site will also be closely scrutinized by the NRC staff.

(b) Situations or relationships. The following situations or relationships may give rise to organizational conflicts of interest:

(1) The offeror or contractor shall disclose information that may give rise to organizational conflicts of interest under the following circumstances. The information may include the scope of work or specification for the requirement being performed, the period of performance, and the name and telephone number for a point of contact at the organization knowledgeable about the commercial contract.

(i) Where the offeror or contractor provides advice and recommendations to the NRC in the same technical area where it is also providing consulting assistance to any organization regulated by the NRC.

(ii) Where the offeror or contractor provides advice to the NRC on the same or similar matter on which it is also providing assistance to any organization regulated by the NRC.

(iii) Where the offeror or contractor evaluates its own products or services, or has been substantially involved in the development or marketing of the products or services of another entity.

(iv) Where the award of a contract would result in placing the offeror or contractor in a conflicting role in which its judgment may be biased in relation to its work for the NRC, or would result in an unfair competitive advantage for the offeror or contractor.

(v) Where the offeror or contractor solicits or performs work at an applicant or licensee site while performing work in the same technical area for the NRC at the same site.

(2) The contracting officer may request specific information from an offeror or contractor or may require special contract clauses such as provided in §2009.570-5(b) in the following circumstances:

(i) Where the offeror or contractor prepares specifications that are to be used in competitive procurements of products or services covered by the specifications.

(ii) Where the offeror or contractor prepares plans for specific approaches or methodologies that are to be incorporated into competitive procurements using the approaches or methodologies.

(iii) Where the offeror or contractor is granted access to information not available to the public concerning NRC plans, policies, or programs that could form the basis for a later procurement action.

(iv) Where the offeror or contractor is granted access to proprietary information of its competitors.

(v) Where the award of a contract might result in placing the offeror or contractor in a conflicting role in which its judgment may be biased in relation to its work for the NRC or might result in an unfair competitive advantage for the offeror or contractor.

(c) Policy application guidance. The following examples are illustrative only and are not intended to identify and resolve all contractor organizational conflict of interest situations.

(1)(i) Example. The ABC Corp., in response to a Request For Proposal (RFP), proposes to undertake certain analyses of a reactor component as called for in the RFP. The ABC Corp. is one of several companies considered to be technically well qualified. In response to the inquiry in the RFP, the ABC Corp. advises that it is currently performing similar analyses for the reactor manufacturer.

(ii) Guidance. An NRC contract for that particular work normally would not be awarded to the ABC Corp. because the company would be placed in a position in which its judgment could be biased in relationship to its work for the NRC. Because there are other well-qualified companies available, there would be no reason for considering a waiver of the policy.

(2)(i) Example. The ABC Corp., in response to an RFP, proposes to perform certain analyses of a reactor component that is unique to one type of advanced reactor. As is the case with other technically qualified companies responding to the RFP, the ABC Corp. is performing various projects for several different utility clients. None of the ABC Corp. projects have any relationship to the work called for in the RFP. Based on the NRC evaluation, the ABC Corp. is considered to be the best qualified company to perform the work outlined in the RFP.

(ii) Guidance. An NRC contract normally could be awarded to the ABC Corp. because no conflict of interest exists which could motivate bias with respect to the work. An appropriate clause would be included in the contract to preclude the ABC Corp. from subsequently contracting for work with the private sector that could create a conflict during the performance of the NRC contract. For example, ABC Corp. would be precluded from the performance of similar work for the company developing the advanced reactor mentioned in the example.

(3)(i) Example. The ABC Corp., in response to a competitive RFP, submits a proposal to assist the NRC in revising NRC's guidance documents on the respiratory protection requirements of 10 CFR Part 20. ABC Corp. is the only firm determined to be technically acceptable. ABC Corp. has performed substantial work for regulated utilities in the past and is expected to continue

similar efforts in the future. The work has and will cover the writing, implementation, and administration of compliance respiratory protection programs for nuclear power plants.

(ii) Guidance. This situation would place the firm in a role where its judgment could be biased in relationship to its work for the NRC. Because the nature of the required work is vitally important in terms of the NRC's responsibilities and no reasonable alternative exists, a waiver of the policy, in accordance with §2009.570-9 may be warranted. Any waiver must be fully documented in accordance with the waiver provisions of this policy with particular attention to the establishment of protective mechanisms to guard against bias.

(4)(i) Example. The ABC Corp. submits a proposal for a new system to evaluate a specific reactor component's performance for the purpose of developing standards that are important to the NRC program. The ABC Corp. has advised the NRC that it intends to sell the new system to industry once its practicability has been demonstrated. Other companies in this business are using older systems for evaluation of the specific reactor component.

(ii) Guidance. A contract could be awarded to the ABC Corp. if the contract stipulates that no information produced under the contract will be used in the contractor's private activities unless this information has been reported to the NRC. Data on how the reactor component performs, which is reported to the NRC by contractors, will normally be disseminated by the NRC to others to preclude an unfair competitive advantage. When the NRC furnishes information about the reactor component to the contractor for the performance of contracted work, the information may not be used in the contractor's private activities unless the information is generally available to others. Further, the contract will stipulate that the contractor will inform the NRC contracting officer of all situations in which the information, developed about the performance of the reactor component under the contract, is proposed to be used.

(5)(i) Example. The ABC Corp., in response to a RFP, proposes to assemble a map showing certain seismological features of the Appalachian fold belt. In accordance with the representation in the RFP and §2009.570-3(b)(1)(i), ABC Corp. informs the NRC that it is presently doing seismological studies for several utilities in the eastern United States, but none of the sites are within the geographic area contemplated by the NRC study.

(ii) Guidance. The contracting officer would normally conclude that award of a contract would not place ABC Corp. in a conflicting role where its judgment might be biased. Section 2052.209-72(c) Work for Others, would preclude ABC Corp. from accepting work which could create a conflict of interest during the term of the NRC contract.

(6)(i) Example. AD Division of ABC Corp., in response to a RFP, submits a proposal to assist the NRC in the safety and environmental review of applications for licenses for the construction, operation, and decommissioning of fuel cycle facilities. ABC Corp. is divided into two separate and distinct divisions, AD and BC. The BC Division performs the same or similar services for industry. The BC Division is currently providing the same or similar services required under the NRC's contract for an applicant or licensee.

(ii) Guidance. An NRC contract for that particular work would not be awarded to the ABC Corp. The AD Division could be placed in a position to pass judgment on work performed by the BC Division, which could bias its work for NRC. Further, the Conflict of Interest provisions apply to ABC Corp. and not to separate or distinct divisions within the company. If no reasonable alternative exists, a waiver of the policy could be sought in accordance with §2009.570-9.

(7)(i) Example. The ABC Corp. completes an analysis for NRC of steam generator tube leaks at one of a utility's six sites. Three months later, ABC Corp. is asked by this utility to perform the same analysis at another of its sites.

(ii) Guidance. Section 2052.290-72(c)(3) would prohibit the contractor from beginning this work for the utility until one year after completion of the NRC work at the first site.

(8)(i) Example. ABC Corp. is assisting NRC in a major on-site analysis of a utility's redesign of the common areas between its twin reactors. The contract is for two years with an estimated value of $5 million. Near the completion of the NRC work, ABC Corp. requests authority to solicit for a $100K contract with the same utility to transport spent fuel to a disposal site. ABC Corp. is performing no other work for the utility.

(ii) Guidance. The Contracting Officer would allow the contractor to proceed with the solicitation because it is not in the same technical area as the NRC work; and the potential for technical bias by the contractor because of financial ties to the utility is slight due to the relative value of the two contracts.

(9)(i) Example. The ABC Corp. is constructing a turbine building and installing new turbines at a reactor site. The contract with the utility is for five years and has a total value of $100 million. ABC Corp. has responded to an NRC Request For Proposal requiring the contractor to participate in a major team inspection unrelated to the turbine work at the same site. The estimated value of the contract is $75K.

(ii) Guidance. An NRC contract would not normally be awarded to ABC Corp. because these factors create the potential for financial loyalty to the utility that may bias the technical judgment of the contractor.

(d) Other considerations.

(1) The fact that the NRC can identify and later avoid, eliminate, or neutralize any potential organizational conflicts arising from the performance of a contract is not relevant to a determination of the existence of conflicts prior to the award of a contract.

(2) It is not relevant that the contractor has the professional reputation of being able to resist temptations which arise from organizational conflicts of interest, or that a follow-on procurement is not involved, or that a contract is awarded on a competitive or a sole source basis.

§2009.570-4 Representation.

(a) The following procedures are designed to assist the NRC contracting officer in determining whether situations or relationships exist which may constitute organizational conflicts of interest with respect to a particular offeror or contractor. The procedures apply to small purchases meeting the criteria stated in the following paragraph (b) of this section.

(b) The organizational conflicts of interest representation provision at §2052.209-71 must be included in solicitations and contracts resulting from unsolicited proposals. The contracting officer must also include this provision for task orders and contract modifications for new work for:

(1) Evaluation services or activities;

(2) Technical consulting and management support services;

(3) Research; and

(4) Other contractual situations where special organizational conflicts of interest provisions are noted in the solicitation and would be included in the resulting contract. This representation requirement also applies to all modifications for additional effort under the contract except those issued under the "Changes" clause. Where, however, a statement of the type required by the organizational conflicts of interest representation provisions has previously been submitted with regard to the contract being modified, only an updating of the statement is required.

(c) The offeror may, because of actual or potential organizational conflicts of interest, propose to exclude specific kinds of work contained in a RFP unless the RFP specifically prohibits the exclusion. Any such proposed exclusion by an offeror will be considered by the NRC in the evaluation of proposals. If the NRC considers the proposed excluded work to be an essential or integral part of the required work and its exclusion would be to the detriment of the competitive posture of the other offerors, the NRC shall reject the proposal as unacceptable.

(d) The offeror's failure to execute the representation required by paragraph (b) of this section with respect to an invitation for bids is considered to be a minor informality. The offeror will be permitted to correct the omission.

§2009.570-5 Contract clauses.

(a) General contract clause. All contracts and simplified acquisitions of the types set forth in §2009.570-4(b) must include the clause entitled, "Contractor Organizational Conflicts of Interest," set forth in §2052.209-72.

(b) Other special contract clauses. If it is determined from the nature of the proposed contract that an organizational conflict of interest exists, the contracting officer may determine that the conflict can be avoided, or, after obtaining a waiver in accordance with §2009.570-9, neutralized through the use of an appropriate special contract clause. If appropriate, the offeror may negotiate the terms and conditions of these clauses, including the extent and time period of any restriction. These clauses include but are not limited to:

(1) Hardware exclusion clauses which prohibit the acceptance of production contracts following a related non-production contract previously performed by the contractor;

(2) Software exclusion clauses;

(3) Clauses which require the contractor (and certain of its key personnel) to avoid certain organizational conflicts of interest; and

(4) Clauses which provide for protection of confidential data and guard against its unauthorized use.

§2009.570-6 Evaluation, findings, and contract award.

The contracting officer shall evaluate all relevant facts submitted by an offeror and other relevant information. After evaluating this information against the criteria of §2009.570-3, the contracting officer shall make a finding of whether organizational conflicts of interest exist with respect to a particular offeror. If it has been determined that real or potential conflicts of interest exist, the contracting officer shall:

(a) Disqualify the offeror from award;

(b) Avoid or eliminate such conflicts by appropriate measures; or

(c) Award the contract under the waiver provision of §2009.570-9.

§2009.570-7 Conflicts identified after award.

If potential organizational conflicts of interest are identified after award with respect to a particular contractor and the contracting officer determines that conflicts do exist and that it would not be in the best interest of the Government to terminate the contract, as provided in the clauses required by §2009.570-5, the contracting officer shall take every reasonable action to avoid, eliminate, or, after obtaining a waiver in accordance with §2009.570-9, neutralize the effects of the identified conflict.

§2009.570-8 Subcontracts.

The contracting officer shall require offerors and contractors to submit a representation statement from all subcontractors (other than a supply subcontractor) and consultants performing services in excess of $10,000 in accordance with §2009.570-4(b). The contracting officer shall require the contractor to include contract clauses in accordance with §2009.570-5 in consultant agreements or subcontracts involving performance of work under a prime contract.

§2009.570-9 Waiver.

(a) The contracting officer determines the need to seek a waiver for specific contract awards with the advice and concurrence of the program office director and legal counsel. Upon the recommendation of the Senior Procurement Executive, and after consultation with legal counsel, the Executive Director for Operations may waive the policy in specific cases if he determines that it is in the best interest of the United States to do so.

(b) Waiver action is strictly limited to those situations in which:

(1) The work to be performed under contract is vital to the NRC program;

(2) The work cannot be satisfactorily performed except by a contractor whose interests give rise to a question of conflict of interest.

(3) Contractual and/or technical review and surveillance methods can be employed by the NRC to neutralize the conflict.

(c) The justification and approval documents for any waivers must be placed in the NRC Public Document Room.

§2009.570-10 Remedies.

In addition to other remedies permitted by law or contract for a breach of the restrictions in this subpart or for any intentional misrepresentation or intentional nondisclosure of any relevant interest required to be provided for this section, the NRC may debar the contractor from subsequent NRC contracts.

Base Period: August 31, 2012 - August 30, 2013					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
0001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
0001A		Financials and Status Reporting	3760		
0001B		Support for Scanning Laptops and Other Tools	1880		
0001C		Quality Assurance for Overall contract Only	1880		
0002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
0002A		Project Manager	3760		
0002B		Program Manager	400		
0003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
0004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
0005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
0006	**Section 8.3.1**	**Authorization**	**EA**		
0006A		Small system (Less than 15 components) - Low Sensitivity	2		
0006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
0006C		Medium system (16-50 components) - Moderate Sensitivity	10		
0006D		Medium system (16-50 components) - High Sensitivity	2		
0006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
0006F		Large system (51-199 or greater components) - High Sensitivity	5		
0007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
0007A		General Use	40		
0007B		SGI	25		
0007C		Classified	10		
0008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	18		
0008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
0008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

0008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
0008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
0008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
0008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
0009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
0009A		Security Engineering Support	3600		
0009B		Process Support	1880		
0010	**Section 8.5**	**Data Calls**	**HR**		
			420		
0011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
0012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
0013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	2		
0013B		Medium system (16-50 components)	4		
0013C		Large system (51-199 components)	2		
0014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
0015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
0016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
0016A		Small system (Less than 10 components tested)	3		
0016B		Medium system (11-60 components tested)	3		
0016C		Large system (60-120 components tested)	1		
0017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
0018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
0019	**Section 8.7.7**	**Communications**	**HR**		
			660		

1020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
0021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
0022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
0023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
0024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
0025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
0026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
0027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
0028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
0029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
0030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 1: August 31, 2013 - August 30, 2014					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
1001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
1001A		Financials and Status Reporting	3760		
1001B		Support for Scanning Laptops and Other Tools	1880		
1001C		Quality Assurance for Overall contract Only	1880		
1002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
1002A		Project Manager	3760		
1002B		Program Manager	400		
1003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
1004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
1005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
1006	**Section 8.3.1**	**Authorization**	**EA**		
1006A		Small system (Less than 15 components) - Low Sensitivity	2		
1006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
1006C		Medium system (16-50 components) - Moderate Sensitivity	10		
1006D		Medium system (16-50 components) - High Sensitivity	2		
1006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
1006F		Large system (51-199 or greater components) - High Sensitivity	5		
1007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
1007A		General Use	40		
1007B		SGI	25		
1007C		Classified	10		
1008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
1008A		Annual Security Controls Test	18		
1008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
1008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

1008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
1008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
1008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
1008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
1009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
1009A		Security Engineering Support	3600		
1009B		Process Support	1880		
1010	**Section 8.5**	**Data Calls**	**HR**		
			420		
1011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
1012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
1013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
1013A		Small system (Less than 15 components)	2		
1013B		Medium system (16-50 components)	4		
1013C		Large system (51-199 components)	2		
1014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
1015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
1016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
1016A		Small system (Less than 10 components tested)	3		
1016B		Medium system (11-60 components tested)	3		
1016C		Large system (60-120 components tested)	1		
1017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
1018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
1019	**Section 8.7.7**	**Communications**	**HR**		
			660		
1020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
1021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
1022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
1023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
1024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
1025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
1026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
1027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
1028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
1029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
1030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 2: August 31, 2014 - August 30, 2015					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
2001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
2001A		Financials and Status Reporting	3760		
2001B		Support for Scanning Laptops and Other Tools	1880		
2001C		Quality Assurance for Overall contract Only	1880		
2002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
2002A		Project Manager	3760		
2002B		Program Manager	400		
2003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
2004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
2005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
2006	**Section 8.3.1**	**Authorization**	**EA**		
2006A		Small system (Less than 15 components) - Low Sensitivity	2		
2006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
2006C		Medium system (16-50 components) - Moderate Sensitivity	10		
2006D		Medium system (16-50 components) - High Sensitivity	2		
2006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
2006F		Large system (51-199 or greater components) - High Sensitivity	5		
2007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
2007A		General Use	40		
2007B		SGI	25		
2007C		Classified	10		
2008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
0008A		Annual Security Controls Test	18		
2008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
2008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

2008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
2008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
2008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
2008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
2009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
2009A		Security Engineering Support	3600		
2009B		Process Support	1880		
2010	**Section 8.5**	**Data Calls**	**HR**		
			420		
2011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
2012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
2013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
2013A		Small system (Less than 15 components)	2		
2013B		Medium system (16-50 components)	4		
2013C		Large system (51-199 components)	2		
2014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
2015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
2016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
2016A		Small system (Less than 10 components tested)	3		
2016B		Medium system (11-60 components tested)	3		
2016C		Large system (60-120 components tested)	1		
2017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
2018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
2019	**Section 8.7.7**	**Communications**	**HR**		
			660		
2020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
2021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
2022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
2023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
2024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
2025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
2026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
2027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
2028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
2029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
2030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 3: August 31, 2015 - August 30, 2016					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
3001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
3001A		Financials and Status Reporting	3760		
3001B		Support for Scanning Laptops and Other Tools	1880		
3001C		Quality Assurance for Overall contract Only	1880		
3002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
3002A		Project Manager	3760		
3002B		Program Manager	400		
3003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
3004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
3005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
3006	**Section 8.3.1**	**Authorization**	**EA**		
3006A		Small system (Less than 15 components) - Low Sensitivity	2		
3006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
3006C		Medium system (16-50 components) - Moderate Sensitivity	10		
3006D		Medium system (16-50 components) - High Sensitivity	2		
3006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
3006F		Large system (51-199 or greater components) - High Sensitivity	5		
3007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
3007A		General Use	40		
3007B		SGI	25		
3007C		Classified	10		
3008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
3008A		Annual Security Controls Test	18		
3008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
3008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

3008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
3008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
3008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
3008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
3009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
3009A		Security Engineering Support	3600		
3009B		Process Support	1880		
3010	**Section 8.5**	**Data Calls**	**HR**		
			420		
3011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
3012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
3013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
3013A		Small system (Less than 15 components)	2		
3013B		Medium system (16-50 components)	4		
3013C		Large system (51-199 components)	2		
3014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
3015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
3016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
3016A		Small system (Less than 10 components tested)	3		
3016B		Medium system (11-60 components tested)	3		
3016C		Large system (60-120 components tested)	1		
3017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
3018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
3019	**Section 8.7.7**	**Communications**	**HR**		
3020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

			660		

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
3021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
3022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
3023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
3024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
3025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
3026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
3027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
3028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
3029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
3030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 4: August 31, 2016 - August 30, 2017					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
4001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
4001A		Financials and Status Reporting	3760		
4001B		Support for Scanning Laptops and Other Tools	1880		
4001C		Quality Assurance for Overall contract Only	1880		
4002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
4002A		Project Manager	3760		
4002B		Program Manager	400		
4003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
4004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
4005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
4006	**Section 8.3.1**	**Authorization**	**EA**		
4006A		Small system (Less than 15 components) - Low Sensitivity	2		
4006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
4006C		Medium system (16-50 components) - Moderate Sensitivity	10		
4006D		Medium system (16-50 components) - High Sensitivity	2		
4006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
4006F		Large system (51-199 or greater components) - High Sensitivity	5		
4007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
4007A		General Use	40		
4007B		SGI	25		
4007C		Classified	10		
4008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
4008A		Annual Security Controls Test	18		
4008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
4008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

4008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
4008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
4008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
4008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
4009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
4009A		Security Engineering Support	3600		
4009B		Process Support	1880		
4010	**Section 8.5**	**Data Calls**	**HR**		
			420		
4011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
4012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
4013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
4013A		Small system (Less than 15 components)	2		
4013B		Medium system (16-50 components)	4		
4013C		Large system (51-199 components)	2		
4014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
4015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
4016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
4016A		Small system (Less than 10 components tested)	3		
4016B		Medium system (11-60 components tested)	3		
4016C		Large system (60-120 components tested)	1		
4017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
4018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
4019	**Section 8.7.7**	**Communications**	**HR**		
			660		
4020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
4021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
4022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
4023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
4024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
4025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
4026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
4027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
4028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
4029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
4030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 5: August 31, 2017 - August 30, 2018					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
5001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
5001A		Financials and Status Reporting	3760		
5001B		Support for Scanning Laptops and Other Tools	1880		
5001C		Quality Assurance for Overall contract Only	1880		
5002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
5002A		Project Manager	3760		
5002B		Program Manager	400		
5003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
5004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
5005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
5006	**Section 8.3.1**	**Authorization**	**EA**		
5006A		Small system (Less than 15 components) - Low Sensitivity	2		
5006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
5006C		Medium system (16-50 components) - Moderate Sensitivity	10		
5006D		Medium system (16-50 components) - High Sensitivity	2		
5006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
5006F		Large system (51-199 or greater components) - High Sensitivity	5		
5007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
5007A		General Use	40		
5007B		SGI	25		
5007C		Classified	10		
5008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
5008A		Annual Security Controls Test	18		
5008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
5008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

5008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
5008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
5008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
5008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
5009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
5009A		Security Engineering Support	3600		
5009B		Process Support	1880		
5010	**Section 8.5**	**Data Calls**	**HR**		
			420		
5011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
5012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
5013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	2		
0013B		Medium system (16-50 components)	4		
0013C		Large system (51-199 components)	2		
5014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
5015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
5016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
5016A		Small system (Less than 10 components tested)	3		
5016B		Medium system (11-60 components tested)	3		
5016C		Large system (60-120 components tested)	1		
5017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
5018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
5019	**Section 8.7.7**	**Communications**	**HR**		
			660		

5020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
5021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
5022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
5023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
5024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
5025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
5026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
5027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
5028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
5029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
5030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 6: August 31, 2018 - August 30, 2019					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
6001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
6001A		Financials and Status Reporting	3760		
6001B		Support for Scanning Laptops and Other Tools	1880		
6001C		Quality Assurance for Overall contract Only	1880		
6002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
6002A		Project Manager	3760		
6002B		Program Manager	400		
6003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
6004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
6005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
6006	**Section 8.3.1**	**Authorization**	**EA**		
6006A		Small system (Less than 15 components) - Low Sensitivity	2		
6006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
6006C		Medium system (16-50 components) - Moderate Sensitivity	10		
6006D		Medium system (16-50 components) - High Sensitivity	2		
6006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
6006F		Large system (51-199 or greater components) - High Sensitivity	5		
6007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
6007A		General Use	40		
6007B		SGI	25		
6007C		Classified	10		
6008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
6008A		Annual Security Controls Test	18		
6008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
6008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

6008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
6008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
6008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
6008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
6009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
6009A		Security Engineering Support	3600		
6009B		Process Support	1880		
6010	**Section 8.5**	**Data Calls**	**HR**		
			420		
6011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
6012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
6013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	2		
0013B		Medium system (16-50 components)	4		
0013C		Large system (51-199 components)	2		
6014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
6015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
6016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
6016A		Small system (Less than 10 components tested)	3		
6016B		Medium system (11-60 components tested)	3		
6016C		Large system (60-120 components tested)	1		
6017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
6018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
6019	**Section 8.7.7**	**Communications**	**HR**		
			660		

6020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
6021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
6022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
6023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
6024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
6025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
6026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
6027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
6028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
6029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
6030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 7: August 31, 2019 - August 30, 2020					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
7001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
7001A		Financials and Status Reporting	3760		
7001B		Support for Scanning Laptops and Other Tools	1880		
7001C		Quality Assurance for Overall contract Only	1880		
7002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
7002A		Project Manager	3760		
7002B		Program Manager	400		
7003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			625		
7004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			1250		
7005	**Section 8.2.4**	**Best Practices**	**HR**		
			650		
7006	**Section 8.3.1**	**Authorization**	**EA**		
7006A		Small system (Less than 15 components) - Low Sensitivity	2		
7006B		Small system (Less than 15 components) - Moderate Sensitivity	10		
7006C		Medium system (16-50 components) - Moderate Sensitivity	10		
7006D		Medium system (16-50 components) - High Sensitivity	2		
7006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
7006F		Large system (51-199 or greater components) - High Sensitivity	5		
7007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
7007A		General Use	40		
7007B		SGI	25		
7007C		Classified	10		
7008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
7008A		Annual Security Controls Test	18		
7008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	3		
7008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	5		

7008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	5		
7008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	3		
7008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
7008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	3		
7009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
7009A		Security Engineering Support	3600		
7009B		Process Support	1880		
7010	**Section 8.5**	**Data Calls**	**HR**		
			420		
7011	**Section 8.6.1**	**Incident Response**	**HR**		
			1880		
7012	**Section 8.6.2**	**Security Architecture**	**HR**		
			940		
7013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
7013A		Small system (Less than 15 components)	2		
7013B		Medium system (16-50 components)	4		
7013C		Large system (51-199 components)	2		
7014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			400		
7015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			850		
7016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
7016A		Small system (Less than 10 components tested)	3		
7016B		Medium system (11-60 components tested)	3		
7016C		Large system (60-120 components tested)	1		
7017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			600		
7018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			750		
7019	**Section 8.7.7**	**Communications**	**HR**		
			660		

7020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $160,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
7021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	1000		
7022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	1500		
7023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	1500		
7024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	800		
7025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	660		
7026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			900		
7027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			300		
7028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	8		
7029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	336		
7030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			500		

Option 8: August 31, 2020 - November 30, 2020					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
8001	**Section 8.0**	**Overall Contract Responsibilities**	**HR**		
8001A		Financials and Status Reporting	940		
8001B		Support for Scanning Laptops and Other Tools	470		
8001C		Quality Assurance for Overall contract Only	470		
8002	**Section 8.1.2**	**Project Plan and Project Manager Support**	**HR**		
8002A		Project Manager	940		
8002B		Program Manager	100		
8003	**Section 8.2.2**	**Classified Processing Support**	**HR**		
			156		
8004	**Section 8.2.3**	**Evaluate New Technology**	**HR**		
			312		
8005	**Section 8.2.4**	**Best Practices**	**HR**		
			156		
8006	**Section 8.3.1**	**Authorization**	**EA**		
8006A		Small system (Less than 15 components) - Low Sensitivity	1		
8006B		Small system (Less than 15 components) - Moderate Sensitivity	2		
8006C		Medium system (16-50 components) - Moderate Sensitivity	2		
8006D		Medium system (16-50 components) - High Sensitivity	1		
8006E		Large system (51-199 or greater components) - Moderate Sensitivity	1		
8006F		Large system (51-199 or greater components) - High Sensitivity	1		
8007	**Section 8.3.2**	**Laptop Authorization**	**EA**		
8007A		General Use	10		
8007B		SGI	6		
8007C		Classified	3		
8008	**Section 8.4**	**Continuous Monitoring Support**	**EA**		
8008A		Annual Security Controls Test	5		
8008B		Continuous Monitoring Activities for a Small System (Less than 15 components) -Low Sensitivity	1		
8008C		Continuous Monitoring Activities for a Small system (Less than 15 components) - Moderate Sensitivity	1		

8008D		Continuous Monitoring Activities for a Medium system (16-50 components) - Moderate Sensitivity	1		
8008E		Continuous Monitoring Activities for a Medium system (16-50 components) - High Sensitivity	1		
8008F		Continuous Monitoring Activities for a Large system (51-199 components) - Moderate Sensitivity	1		
8008G		Continuous Monitoring Activities for a Large system (51-199 components) - High Sensitivity	1		
8009	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
8009A		Security Engineering Support	900		
8009B		Process Support	470		
8010	**Section 8.5**	**Data Calls**	**HR**		
			105		
8011	**Section 8.6.1**	**Incident Response**	**HR**		
			470		
8012	**Section 8.6.2**	**Security Architecture**	**HR**		
			235		
8013	**Section 8.6.3**	**Vulnerability Assessment**	**EA**		
0013A		Small system (Less than 15 components)	2		
0013B		Medium system (16-50 components)	4		
0013C		Large system (51-199 components)	2		
8014	**Section 8.6.4**	**Source Code Reviews**	**HR**		
			100		
8015	**Section 8.6.5**	**Penetration Testing**	**HR**		
			212		
8016	**Section 8.6.6**	**Security Impact Assessments**	**EA**		
8016A		Small system (Less than 10 components tested)	1		
8016B		Medium system (11-60 components tested)	1		
8016C		Large system (60-120 components tested)	1		
8017	**Section 8.7.1**	**Cyber Security Policy**	**HR**		
			150		
8018	**Section 8.7.2**	**Processes, Procedures, Templates, Checklists, Standards, and Guidance**	**HR**		
			188		
8019	**Section 8.7.7**	**Communications**	**HR**		
			165		
8020	**N/A**	**Other Direct Costs**	**HR**	N/A	Not to Exceed $40,000.00.

OPTIONAL CLINs					
Contract Line Item Number (CLIN)	**SOW Cross Reference**	**Description**	**Unit**	**Unit Price**	**Ceiling Price**
8021	**Section 8.2.1**	**Residual Risk per system**	**HR**		
		Special systems (infrastructure)	250		
8022	**Section 8.3.1**	**Authorization**	**HR**		
		Special system (At least 200 components)	375		
8023	**Section 8.4**	**Continuous Monitoring Support**	**HR**		
		Special system (At least 200 components)	375		
8024	**Section 8.6.3**	**Vulnerability Assessment**	**HR**		
		Special system (At least 200 components)	200		
8025	**Section 8.6.6**	**Security Impact Assessments**	**HR**		
		Special system (121 or more components tested)	165		
8026	**Section 8.7.3**	**Cyber Security Relevant Business Solutions**	**HR**		
			225		
8027	**Section 8.7.4**	**Cyber Security Awareness Training**	**HR**		
			75		
8028	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**EA**		
		Course Development per day	2		
8029	**Section 8.7.5**	**Cyber Security Role Based Awareness Training (development and instruction)**	**HR**		
		Instruction per day (42 days)	85		
8030	**Section 8.7.6**	**Cyber Security Conference**	**HR**		
			125		