

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>			1. CONTRACT ID NO.	PAGE OF PAGES	
				1	4

2. AMENDMENT/MODIFICATION NO. 003	3. EFFECTIVE DATE 11/26/07	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (if applicable)
--------------------------------------	-------------------------------	----------------------------------	--------------------------------

6. ISSUED BY National Heart, Lung, and Blood Institute Rockledge II Building, Room 6016 6701 Rockledge Drive, MSC 7902 Bethesda, MD 20892-7902	CODE	7. ADMINISTERED BY (if other than Item 6)  See Block 6	CODE
--	------	--	------

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(✓)	9A. AMENDMENT OF SOLICITATION NO. NHLBI-HR-08-06
	X	9B. DATED (SEE ITEM 13) 11/26/07
		10A. MODIFICATION OF CONTRACT/ ORDER NO.
		10B. DATED (SEE ITEM 13)
CODE	FACILITY CODE	

**11. THIS ITEM APPLIES TO AMENDMENTS OF SOLICITATIONS**

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers  is extended,  is not extended.  
Offerors 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 1 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 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.**

(✓)	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 data, 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  is not,  is required to sign this document and return 1 copies to the issuing office.

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

The purpose of this amendment is to replace in its entirety, Section L, item 2.b.11. Information Security found on pages 48 to 51. See the following SF 30 Continuation Pages.

All other terms and conditions of this solicitation remain unchanged.

Except as provided herein, all items 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) Joanne Deshler, Contracting Officer
15B. CONTRACTOR/OFFEROR	16B. UNITED STATES OF AMERICA
15C. DATE SIGNED	16C. DATE SIGNED 11/26/2007
(Signature of person authorized to sign.)	BY _____ /S/ _____ (Signature of Contracting Officer)

**SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS**

**2. INSTRUCTIONS TO OFFERORS**

**b. TECHNICAL PROPOSAL INSTRUCTIONS**

11. Information Security is applicable to this solicitation and the following information is provided to assist in proposal preparation.

**IMPORTANT NOTE TO OFFERORS:** The following information shall be addressed in a separate section of the Technical Proposal entitled, "INFORMATION SECURITY."

The Federal Information Security Management Act of 2002 (P.L. 107-347) (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to safeguard information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor (including subcontractor), or other source. The National Institute of Standards and Technology (NIST) has issued a number of publications that provide guidance in the establishment of minimum security controls for management, operational and technical safeguards needed to protect the confidentiality, integrity and availability of a Federal information system and its information.

The Statement of Work (SOW) requires the successful offeror to (1) develop, (2) have the ability to access, or (3) host and/or maintain a Federal information system(s). Pursuant to Federal and HHS Information Security Program Policies the following requirements apply to this solicitation:

Federal Information Security Management Act of 2002 (FISMA), Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002); <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>

a. Information Type

Administrative, Management and Support Information:

Mission Based Information:

b. Security Categories and Levels

Confidentiality Level:       Low  Moderate  High  
Integrity Level:             Low  Moderate  High  
Availability Level:         Low  Moderate  High  
**Overall Level:**             Low  Moderate  High

c. Position Sensitivity Designations

Prior to award, the Government will determine the position sensitivity designation for each Contractor (including subcontractor) employee that the successful offeror proposes for work under the contract. For proposal preparation purposes, the following designations apply:

[X] Level 5: Public Trust - Moderate Risk (Requires Suitability Determination with NACIC, MBI or LBI). Contractor employees assigned to a Level 5 position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI) Upon award, the Contractor will be required to submit a roster of all staff (including subcontractor staff) working under the contract who will develop, have the ability to access, or host and/or maintain a federal information system(s). The Government will determine and notify the Contractor of the appropriate level of suitability investigation required for each staff member. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for Contractor use at: <http://ais.nci.nih.gov/forms/Suitability-roster.xls>

Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification. Additional submission instructions can be found at the "NCI Information Technology Security Policies, Background Investigation Process" website: <http://ais.nci.nih.gov> .

Contractor/Subcontractor employees who have met investigative requirements within the past five years may only require an updated or upgraded investigation.

d. Information Security Training

HHS policy requires Contractors/Subcontractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.

The successful offeror will be responsible for assuring that each Contractor/Subcontractor employee has completed the NIH Computer Security Awareness Training course at: <http://irtsectraining.nih.gov/> prior to performing any contract work, and thereafter completing the NIH-specified fiscal year refresher course during the period of performance of the contract. The successful offeror shall maintain a listing of all individuals who have completed this training and shall submit this listing to the Project Officer.

Additional security training requirements commensurate with the position may be required as defined in NIST Special Publication 800-16, Information Technology Security Training Requirements ( <http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf> ). This document provides information about information security training that may be useful to potential offerors.

e. Offeror's Official Responsible for Information Security

The offeror shall include in the "Information Security" part of its Technical Proposal the name and title of its official who will be responsible for all information security requirements should the offeror be selected for an award.

f. NIST SP 800 53 Self Assessment

The offeror must include in the "Information Security" part of its Technical Proposal, a completed Self-Assessment required by NIST Draft SP 800-53, Recommended Security Controls for Federal Information Systems. ( <http://csrc.nist.gov/publications> - under Special Publications).

Subcontracts : The offeror must include similar information for any proposed subcontractor that will perform under the SOW to (1) develop a Federal information system(s) at the offeror's/subcontractor's facility, or (2) host and/or maintain a Federal information system(s) at the offeror's/subcontractor's facility.

g. Draft Information System Security Plan

The offeror must include a draft Information System Security Plan (ISSP) using the current template in Appendix A of NIST SP 800 18, Guide to Developing Security Plans for Federal Information Systems (<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>). The details contained in the offeror's draft ISSP must be commensurate with the size and complexity of the requirements of the SOW based on the System Categorization determined above in subparagraph (b) Security Categories and Levels.

Subcontracts : The offeror must include similar information for any proposed subcontractor that will perform under the SOW with the offeror whenever the submission of an ISSP is required.

Note to Offeror: The resultant contract will require the draft ISSP to be finalized in coordination with the Project Officer no later than 90 calendar days after contract award. Also, a contractor is required to update and resubmit its ISSP to NIH every three years following award or when a major modification has been made to its internal system.

h. References

1. Federal Information Security Management Act of 2002 (FISMA), Title III, E-Government Act of 2002, Pub. L. No. 107-347 (Dec. 17, 2002); <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf>
2. DHHS Personnel Security/Suitability Handbook: <http://www.hhs.gov/ohr/manual/pssh.pdf>
3. NIH Computer Security Awareness Training Course: <http://irtsectraining.nih.gov/>

The following NIST publications may be found at the following site: <http://csrc.nist.gov/publications/>  
[Note: The search tool on the left side of this page provides easy access to the documents.]

4. NIST Special Publication 800-16, Information Technology Security Training Requirements; and Appendix A-D
5. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
6. NIST SP 800-26, Revision 1, Computer Security
7. NIST SP 800-53, Revision 1, Recommended Security Controls for Federal Information Systems
8. NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I; and Volume II, Appendices to Guide For Mapping Types of Information and Information Systems To Security Categories, Appendix C, and Appendix D
9. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle
10. FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
11. FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems