OFFICE OF ACQUISITIONS
NATIONAL CANCER INSTITUTE

REQUEST FOR PROPOSAL NUMBER: N02CP81015-49

Amendment No.: 1

Date of Issuance: March 12, 2008

The above numbered Request For Proposal (RFP) is amended as set forth below. The hour and date specified for receipt of Offerors remains unchanged, 2:00 PM local time on April 7, 2008.

Offerors MUST acknowledge receipt of the amendment prior to the hour and the date specified in the solicitation or as amended, by separate letter, telegram, or Electronic Mail which includes a reference to the RFP and Amendment number(s). For your convenience, the Proposal Intent Response Form is provided in SECTION J - List of Attachments of this RFP, for this purpose.

FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERORS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.

This Amendment revises the RFP as stated below:

PART I, SECTION H - SPECIAL CONTRACT REQUIREMENTS, ARTICLE H.10. INFORMATION SECURITY, paragraphs a., b., and c., are amended to provide the applicable security levels, as follows:

The Statement of Work (SOW) requires the Contractor 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 Contractor and any subcontractor performing under this contract shall comply with the following requirements:

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

[X] Mission Based Information

D.14.3 Public Health Monitoring
D.20.1 Research and Development
D.20.2 General Purpose Data and Statistics

b. Security Categories and Levels

Confidentiality Level: [ ] Low [X] Moderate [ ] High
Integrity Level: [ ] Low [X] Moderate [ ] High
Availability Level: [ ] Low [X] Moderate [ ] High

Overall Level: [ ] Low [X] Moderate [ ] High

c. Position Sensitivity Designations

1. The following position sensitivity designations and associated clearance and investigation requirements apply under this contract.

[ ] Level 6: Public Trust - High Risk (Requires Suitability Determination with a BI). Contractor employees assigned to a Level 6 position are subject to a Background Investigation (BI)

[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).

[X] Level 1: Non Sensitive (Requires Suitability Determination with an NACI). Contractor employees assigned to a Level 1 position are subject to a National Agency Check and Inquiry Investigation (NACI).

2. The Contractor shall submit a roster, by name, position, e-mail address, phone number and responsibility, 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 roster shall be submitted to the Project Officer, with a copy to the Contracting Officer, within 14 calendar days of the effective date of the contract. Any revisions to the roster as a result of staffing changes shall be submitted within 15 calendar days of the change. The Contracting Officer shall notify the Contractor of the appropriate level of suitability investigations to be performed. 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.

3. Contractor/Subcontractor employees shall comply with the HHS criteria for the assigned position sensitivity designations prior to performing any work under this contract. The following exceptions apply:

Levels 5 and 1: Contractor/Subcontractor employees may begin work under the contract after the Contractor has submitted the name, position and responsibility of the employee to the Project Officer, as described in paragraph c. (2) above.

Level 6: In special circumstances the Project Officer may request a waiver of the pre-appointment investigation. If the waiver is granted, the Project Officer will provide written authorization for the Contractor/Subcontractor employee to work under the contract.

d. Information Security Training

The Contractor shall ensure 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 Contractor shall maintain a listing by name and title of each Contractor/Subcontractor employee working under this contract that has completed the NIH required training. Any additional security training completed by Contractor/ Subcontractor staff shall be included on this listing. [The listing of completed training shall be included in the first technical progress report. (See Article C.2. Reporting Requirements.) Any revisions to this listing as a result of staffing changes shall be submitted with next required technical progress report.]

e. Rules of Behavior

The Contractor/Subcontractor employees shall comply with the NIH Information Technology General Rules of Behavior at: http://irm.cit.nih.gov/security/nihitrob.html.

f. Personnel Security Responsibilities

Contractor Notification of New and Departing Employees Requiring Background Investigations

1. The Contractor shall notify the Contracting Officer, the Project Officer, and the Security Investigation Reviewer **within five working days** before a new employee assumes a position that requires a suitability determination or when an employee with a security clearance stops working under the contract. The Government will initiate a background investigation on new employees requiring security clearances and will stop pending background investigations for employees that no longer work under the contract.

2. New employees: Provide the name, position title, e-mail address, and phone number of the new employee. Provide the name, position title and suitability level held by the former incumbent. If the employee is filling a new position, provide a description of the position and the Government will determine the appropriate security level.

3. Departing employees:

- Provide the name, position title, and security clearance level held by or pending for the individual.
- Perform and document the actions identified in the "Employee Separation Checklist", attached in Section J, ATTACHMENTS of this contract, when a Contractor/Subcontractor employee terminates work under this contract. All documentation shall be made available to the Project Officer and/or Contracting Officer upon request.

g. Commitment to Protect Non-Public Departmental Information Systems and Data

1. Contractor Agreement

The Contractor and its subcontractors performing under this SOW shall not release, publish, or disclose non-public Departmental information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of such information:

-18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
-18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
-Public Law 96-511 (Paperwork Reduction Act)

2. Contractor-Employee Non-Disclosure Agreements

Each Contractor/Subcontractor employee who may have access to non-public Department information under this contract shall complete the Commitment to Protect Non-Public Information - Contractor Agreement. A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer prior to performing any work under the contract.

h. NIST SP 800-53 Self-Assessment

The contractor shall annually update and re-submit its Self-Assessment required by NIST SP 800-53, Recommended Security Controls for Federal Information Systems. (http://csrc.nist.gov/publications - under Special Publications).

Subcontracts: The Contractor's annual update to its Self-Assessment Questionnaire shall include similar information for any subcontractor that performs under the SOW to (1) develop a Federal information system(s) at the Contractor's/ Subcontractor's facility, or (2) host and/or maintain a Federal information system(s) at the Contractor's/Subcontractor's facility.

The annual update shall be submitted to the Project Officer, with a copy to the Contracting Officer [For option contracts: no later than the completion date of the period of performance/ for all other contracts: indicate due date as determined by the Project Officer/Contracting Officer].

i. Information System Security Plan

The Contractor's draft ISSP submitted with its proposal shall be finalized in coordination with the Project Officer no later than 90 calendar days after contract award.

Following approval of its draft ISSP, the Contractor shall update and resubmit its ISSP to the Project Officer every three years or when a major modification has been made to its internal system. The Contractor shall use the current

ISSP 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 Contractor's ISSP shall 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 of this Article.

Subcontracts: The Contractor shall include similar information for any subcontractor performing under the SOW with the Contractor whenever the submission of an ISSP is required.

SECTION L - INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS, Section 2. INSTRUCTIONS TO OFFERORS, paragraph b. Technical Proposal Instructions, **Additional Technical Evaluation Proposal Information Specific To This Solicitation**, Item 15 Information Security, is amended to provide the applicable security levels, as follows:

15. 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:

[X]Mission Based Information:

D.14.3 Public Health Monitoring
D.20.1 Research and Development
D.20.2 General Purpose Data and Statistics

b. Security Categories and Levels

Confidentiality Level: [ ] Low [X] Moderate [ ] High
Integrity Level: [ ] Low [X] Moderate [ ] High
Availability Level: [ ] Low [X] Moderate [ ] High

Overall Level: [ ] Low [X] 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:

[ ] Level 6: Public Trust - High Risk (Requires Suitability Determination with a BI). Contractor employees assigned to a Level 6 position are subject to a Background Investigation (BI).

[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)

[X] Level 1: Non Sensitive (Requires Suitability Determination with an NACI). Contractor employees assigned to a Level 1 position are subject to a National Agency Check and Inquiry Investigation (NACI).

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

ALL OTHER TERMS AND CONDITIONS REMAIN UNCHANGED