AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 | 7

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
Master Mod 001	See Block 16C.		

6. ISSUED BY CODE

National Institutes of Health
Division of Information Technology Acquisitions
6011 Executive Boulevard, Suite 503 J
Rockville, Maryland 20852

7. ADMINISTERED BY (If other than Item 6) CODE

OMB No. 0990-0115

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

Image World2 nd Prime Vendors

CODE | FACILITY CODE

(X) X

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED (SEE ITEM 13) December 21, 2000

11. THIS ITEM ONLY 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.

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 CONTACT/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:
X	D. OTHER (Specify type of modification and authority) Change FAR 52.243-1

E. IMPORTANT: Contractor [X] is not, [ ] is required to sign this document and return N/A 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 modification is to revise Article H.7 - Security, and replace with the revised Article H.7 - Security (Revision 1), to include the following DHHS Information Technology Security Provisions:

H.7.1 - Information Technology Security
H.7.2 - Confidential Treatment of Sensitive Information
H.7.3 - Information Technology Systems Security Specifications

(All other Terms and Conditions remain unchanged)

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remain 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)	
		Donald A. Wilson, Sr. Contracting Officer	
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 OCT 21, 2004

H.7 SECURITY (Revision 1)

This document is unclassified; however, the classification of the work to be performed on specific task orders and delivery orders issued under this contract may require security clearances. In that event, the contractor will be advised of the requirements in the task order SOW or The contractor shall follow conscientiously the security requirements identified in documents and other guidance that may be established by the AMO/COTR.

H.7.1 Information Technology Systems Security

Provision H.7.1 is applicable to DHHS task orders and delivery orders involving, in whole or in part, information technology (IT) where the contractor will develop or have access to an automated information system (AIS), and the order is subject to the security requirements of the DHHS Automated Information Systems Security Program (AIISP). The task order SOW or delivery order security attachment will include this provision complete with order-specific information when applicable.

(a) Sensitivity and Security Level Designations.

The Statement of Work (SOW) requires the successful offeror to develop or access a Federal Automated Information System (AIS). Based upon the security guidelines contained in the *Department of Health and Human Services (DHHS) Automated Information Systems Security Program (AISSP) Handbook,* the Government has determined that the following apply:

(1) Category of Safeguarded Information

The safeguarded agency information that the successful offeror will develop or access is categorized as:

[ ] Non Sensitive Information
[ ] Sensitive Information
[ ] Classified Information:
[ ] Confidential [ ] Secret
[ ] Top Secret [ ] Special Access

(2) Security Level Designations

The information that the successful offeror will develop or access is designated as follows:

Level ___ applies to the sensitivity of the data.
Level ___ applies to the operational criticality of the data.

The overall Security Level designation for this requirement is **Level ___**.

(3) Position Sensitivity Designations

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

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

[ ] **Level 5C: Sensitive - Moderate Risk (Requires Suitability Determination with NACIC).**
Contractor employees assigned to a Level 5C position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), or possibly a Limited Background Investigation (LBI).

[ ] **Level 4C: Classified (Requires Special Access Clearance with an SSBI)**.
Contractor employees assigned to a Level 4C position are subject to a Single Scope Background Investigation (SSBI).

[ ] **Level 3C: Classified (Requires Top Secret Clearance with an SSBI).**
Contractor employees assigned to a Level 3C position are subject to a Single Scope Background Investigation (SSBI).

[ ] **Level 2C: Classified (Requires Confidential or Secret Clearance with an LBI).**
Contractor employees assigned to a Level 2C position shall undergo a Limited Background Investigation (LBI).

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

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

(b) Information Technology (IT) System Security Program

The offeror's proposal must:

(1) Include a detailed outline (commensurate with the size and complexity of the requirements of the SOW) of its present and proposed IT systems security program;

(2) Demonstrate that it complies with the AISSP security requirements, the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems;" and the DHHS AISSP Handbook.

At a minimum, the offeror's proposed information technology (IT) systems security program must address the minimum requirements of a **Security Level __*__** identified in the DHHS AISSP Handbook, Exhibit III-A, Matrix of Minimum Security Safeguards (http://rcb.cancer.gov/rcb-internet/wkf/IT-security-exhibitIII.pdf)

(3) Include an acknowledgment of its understanding of the security requirements.

(4) Provide similar information for any proposed subcontractor developing or accessing an AIS.

(c) Required Training for IT Systems Security

DHHS policy requires that contractors 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 employee has completed the Computer Security Awareness Training as specified in task/delivery orders prior to performing any contract work. The contractor will be required to maintain a listing of all individuals who have completed this training and submit this listing to the Government.

*** (**NOTE:** Include below when a prospective offeror will require access to sensitive information in order to prepare an offer, e.g. an offeror must access an NIH computer room floor plan. If this is not applicable to your solicitation, delete the entire subparagraph (d) below.) ***

(d) Prospective Offeror Non-Disclosure Agreement

The Government has determined that prospective offerors will require access to sensitive information described below in order to prepare an offer.

*** (**NOTE:** Provide a description of the sensitive information and select the appropriate Position Sensitivity designation.) ***

Any individual having access to this information must possess a valid and current suitability determination at the following level:

[ ] Level 6C: Sensitive - High Risk
[ ] Level 5C: Sensitive - Moderate Risk

To be considered for access to this sensitive information, a prospective offeror must:

(1) Submit a written request to the Contracting Officer identified in the solicitation;
(2) Complete and submit the "Prospective Offeror Non-Disclosure Agreement" available on the NITAAC Website; and
(3) Receive written approval from the Contracting Officer.

Prospective offerors are required to process their requests for access, receive Government approval, and then access the sensitive information within the period of time provided in the solicitation for the preparation of offers.

Nothing in this provision shall be construed, in any manner, by a prospective offeror as an extension to the stated date, time, and location in the solicitation for the submission of offers.

(e) References

The following documents are electronically accessible:

(1) OMB Circular A-130, Appendix III: http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html
(2) DHHS AISSP Handbook: http://irm.cit.nih.gov/policy/aissp.html
(3) DHHS Personnel Security/Suitability Handbook: http://www.hhs.gov/ohr/manual/pssh.pdf
(4) NIH Applications/Systems Security Template: http://cit.nih.gov/security/secplantemp.html
(5) NIST Special Publication 800-16, "Information Technology Security Training Requirements:" http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
(6) NIH CIT-Policies, Guidelines and Regulations:

Table 1-Categories of Safeguarded Agency Information: http://irm.cit.nih.gov/security/table1.htm
Table 2 - Security Level Designations for Agency Information: http://irm.cit.nih.gov/security/table2.htm
Table 3 - Positions Sensitivity Designations for Individuals Accessing Agency Information: http://irm.cit.nih.gov/security/table3.htm

H.7.2 Confidential Treatment of Sensitive Information

Provision H.7.2 is applicable to DHHS task orders and delivery orders where the contractor will have access to sensitive information/data during the performance of the order that needs to be handled confidentially by the contractor, but including the clause at HHSAR352.224-70, Confidentiality of Information, would be inappropriate. The task order SOW or delivery order security attachment will include this provision when applicable.

The Contractor shall guarantee strict confidentiality of the information/data that it is provided by the Government during the performance of the contract. The Government has determined that the information/data that the Contractor will be provided during the performance of the contract is of a sensitive nature.

Disclosure of the information/data, in whole or in part, by the Contractor can only be made after the Contractor receives prior written approval from the Contracting Officer. Whenever the Contractor is uncertain with regard to the proper handling of information/data under the contract, the Contractor shall obtain a written determination from the Contracting Officer.

H.7.3 Information Technology Systems Security Specifications

Provision H.7.3 is applicable to DHHS task orders and delivery orders involving, in whole or in part, IT where the contractor will develop or have access to AIS, and the order is subject to the security requirements of the DHHS AIISP. The task order SOW or delivery order security attachment will include this provision complete with order-specific information when applicable.

The contractor agrees to comply with the IT systems security and/or privacy specifications set forth herein; the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the DHHS Automated Information Systems Security Program (AISSP) Handbook, which may be found at the following websites:

Computer Security Act of 1987: **http://csrc.nist.gov/ispab/csa_87.txt**
OMB A-130, Appendix III: **http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html**
DHHS AISSP Handbook: **http://irm.cit.nih.gov/policy/aissp.html**

The contractor further agrees to include this provision in any subcontract awarded pursuant to this prime contract. Failure to comply with these requirements shall constitute cause for termination.

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of the SOW. The contractor shall establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive Government information, data, and/or equipment.

In addition, during all activities and operations on Government premises, the contractor shall comply with DHHS, including Operational Division, rules of conduct.

a. Required IT Systems Security Training

The contractor shall assure that each employee has completed the Computer Security Awareness Training as specified in task/delivery orders prior to performing any work.

The contractor shall maintain a listing by name and title of each individual working under task/delivery orders that has completed the required security training. Any additional security training completed by contractor staff shall be included on this listing. The listing of completed training and any revisions shall be delivered to the Government as specified in task/delivery orders.

b. Position Sensitivity Designations

The Government has determined that the following position sensitivity designations and associated clearance and investigation requirements apply under this contract:

*** (NOTE: The position sensitivity designations below are to be finalized following review of proposals and prior to task order award.) ***

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

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 5C: Sensitive - Moderate Risk (Requires Suitability Determination with NACIC).
Contractor employees assigned to a Level 5C position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), or possibly a Limited Background Investigation (LBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 4C: Classified (Requires Special Access Clearance with an SSBI).
Contractor employees assigned to a Level 4C position are subject to a Single Scope Background Investigation (SSBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 3C: Classified (Requires Top Secret Clearance with an SSBI).
Contractor employees assigned to a Level 3C position are subject to a Single Scope Background Investigation (SSBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 2C: Classified (Requires Confidential or Secret Clearance with an LBI).
Contractor employees assigned to a Level 2C position shall undergo a Limited Background Investigation (LBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

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

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Contractor employees in AIS-related positions shall comply with the DHHS criteria for the assigned position sensitivity designations prior to performing any work under this contract.

Contractor employees who have met investigative requirements within the past five years may only require an updated or upgraded investigation. Verifications of completed investigations (e.g. copies of certificates of investigations or security clearances), as well as requests for new investigations, shall be submitted to the Project Officer.

c. Commitment to Protect Sensitive Information

(1) Contractor Agreement

The Contractor shall not release, publish, or disclose sensitive 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 sensitive 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 employee who may have access to sensitive information under this delivery order shall complete the "Contractor Employee Non-Disclosure Agreement" available on the NITAAC Website.

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.