IW2*nd* Delivery Order Security Attachment

Delivery Order Title: _____
Delivery Order Tracking No.: _____

This Delivery Order Security Attachment is designed specifically for NITAAC's Department of Health and Human Services (HHS) customers and is based on guidance found in the HHS Information Security Program Policy at: http://intranet.hhs.gov/infosec/docs/policies_guides/ISPP/Information_Security_Program_Policy.pdf

Non-HHS customers should prepare delivery orders in a manner compliant with the security requirements and guidance of their agencies.

THIS DELIVERY ORDER SECURITY ATTACHMENT IS REQUIRED FOR HHS DELIVERY ORDERS IN WHICH CONTRACTOR/SUBCONTRACTOR PERSONNEL WILL (1) DEVELOP, (2) HAVE THE ABILITY TO ACCESS, OR (3) HOST AND/OR MAINTAIN A FEDERAL INFORMATION SYSTEM(S).

The general applicability of this Delivery Order Security Attachment is summarized by IW2nd Contract Line Item (CLIN) category in Table 1, below.

The specific applicability of each security attachment section is clarified in the instructions at the beginning of each section.

If unclear about the applicability of this attachment to your delivery order, consult your Information Systems Security Officer (ISSO), Project Officer (PO), or NITAAC contracting officer.

Note: Italics are used to provide guidance, while normal font in used to provide suggested content. ***Please delete all guidance when finalizing this security attachment.***

Table 1. Applicability of this Security Attachment to IW2nd Delivery Orders

CLIN Category	***Applicability of Security Attachment***
1. COTS Hardware Acquisitions	*Not likely, as these categories generally do not involve contractor access to an AIS or to sensitive information*
2. COTS Software Acquisitions	
3. Integrated Systems, Services, and Solutions (ISSS)	*Likely, as this category may involve software or system installation, customization, or modification; definition of IT operational procedures; etc.*
4. Personnel Services (Labor)	*CLIN category 4 is not applicable to delivery orders*

1. Security Provisions

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

This Delivery Order (DO) 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 task order 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

Based on the recommendation of the ISSO and PO, select the appropriate general information type(s) below, and provide the specific type of information.

[ ] Administrative, Management and Support Information:

Insert specific type of information from NIST SP 800-60, Volume II: Appendices to Guide For Mapping Types Of Information and Information Systems To Security Categories, APPENDIX C at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf.

[ ] Mission Based Information:

Insert specific type of information from NIST SP 800-60, Volume II: Appendices to Guide For Mapping Types Of Information and Information Systems To Security Categories, APPENDIX D at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf.

b. Security Categories and Levels

In coordination with the ISSO, select the Security Level for each Security Category. Select the Overall Security Level which is the highest level of the three factors (Confidentiality, Integrity and Availability). NIST SP 800-60, Volume II: Appendices to Guide For Mapping Types of Information and Information Systems to Security Categories, Appendices C and D contain suggested Security Levels for Each Information Type at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf.

For additional information and assistance for completion of this item, See Table 1, Security Categorization of Federal Information and Information Systems at: http://irm.cit.nih.gov/security/table1.htm.

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

c. Position Sensitivity Designations

(1) The following position sensitivity designations and associated clearance and investigation requirements apply under this task order.

Check all that apply. Delete those that do not apply. If more than one of the below designations apply to the task order, the Contracting Officer (CO), PO and ISSO may wish to consider whether there is a need to identify specific Contractor Position Titles with the applicable sensitivity designations. Additional Note: Levels 2, 3, and 4 are reserved for National Security positions which are generally not applicable to NIH.

For additional information and assistance for completion of this item, See Table 2, Position Sensitivity Designations for Individuals Accessing Agency Information at: http://irm.cit.nih.gov/security/table2.htm.

[ ] 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).

List applicable Contractor Position Titles here if considered appropriate following review of proposals and prior to award.

[ ] 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).

List applicable Contractor Position Titles here if considered appropriate following review of proposals and prior to award.

[ ] 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).

List applicable Contractor Position Titles here if considered appropriate following review of proposals and prior to award.

(2) The contractor shall submit a roster, by name, position and responsibility, of all staff (including subcontractor staff) working under the task order 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 task order. 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.

The last sentence in the paragraph below may be deleted for ICs other than National Cancer Institute (NCI) who do not wish to refer to the NCI web page. The sentence may also be revised to tailor the information to another Institute/Center (IC) web page as desired. It is noted that this reference page is available for other IC contracting offices to use if desired by the IC.

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 task order. The following exceptions apply:

Levels 5 and 1: Contractor/subcontractor employees may begin work under the task order after the contractor has submitted the name, position and responsibility of the employee to the Project Officer, as described in subparagraph 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 task order.

d. Information Security Training

For non-NIH requirements, modify the following paragraph to specify the appropriate information security awareness training course.

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 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 task order work, and thereafter completing the NIH-specified fiscal year refresher course during the period of performance of the task order.

The language contained within the brackets in the paragraph below is suggested only. The CO may choose to require this listing to be submitted separately or in another manner. The only requirement is that this listing must be submitted to the Project Officer as well as the Contracting Officer. If you choose to require this as a separate report, make sure that the DO provides specific instructions on the submission of the report.

The contractor shall maintain a listing by name and title of each contractor/subcontractor employee working under this task order 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. Any revisions to this listing as a result of staffing changes shall be submitted with next required technical progress report.]

If the Government will require contractor/subcontractor staff to take additional security training, include the following paragraph with a listing of the additional training requirements/courses. Otherwise, delete the paragraph in its entirety.

Contractor/subcontractor staff shall complete the following additional training prior to performing any work under this contract:

List the required training courses here.

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. Rules of Behavior

For non-NIH requirements, modify the following paragraph to specify the appropriate information technology 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.

g. Personnel Security Responsibilities

The contractor shall perform and document the actions identified in the "Employee Separation Checklist" (http://nitaac.nih.gov/downloads/iw2/Employee_Separation_Checklist.doc) 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.

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

(1) Contractor Agreement

The Contractor and its subcontractors performing under this DO 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 task order 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.

INCLUDE SECTION i, BELOW, WHEN THE DO REQUIRES THE CONTRACTOR/SUBCONTRACTOR 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.

For additional information and assistance for completion of this item, See Table 3, Federal Information Security Safeguard Requirements-Summary at: http://irm.cit.nih.gov/security/table3.htm.

i. 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 DO 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.

Indicate when the annual update is due. If one of the choices within the brackets below is not appropriate for your task order situation, modify the sentence below as necessary.

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].

INCLUDE SECTION j, BELOW, WHEN:

1. THE DO REQUIRES THE CONTRACTOR/SUBCONTRACTOR TO DEVELOP A FEDERAL INFORMATION SYSTEM(S) AT THE CONTRACTOR'S/SUBCONTRACTOR'S FACILITY AND THE PROJECT OFFICER AND INFORMATION SYSTEMS SECURITY OFFICER REQUIRE THE SUBMISSION OF AN INFORMATION SYSTEM SECURITY PLAN;

OR

2. THE DO REQUIRES THE CONTRACTOR/SUBCONTRACTOR TO HOST AND/OR MAINTAIN A FEDERAL INFORMATION SYSTEM(S) AT THE CONTRACTOR'S/SUBCONTRACTOR'S FACILITY.

For additional information and assistance for completion of this item, See Table 3, Federal Information Security Safeguard Requirements-Summary at: http://irm.cit.nih.gov/security/table3.htm.

Make sure to appropriately designate the subparagraph below.

j. 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 task order 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 DO 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 DO with the contractor whenever the submission of an ISSP is required.

INCLUDE SECTION k, BELOW, ONLY IF A PROSPECTIVE OFFEROR WILL REQUIRE ACCESS TO SENSITIVE FEDERAL INFORMATION IN ORDER TO PREPARE AN OFFER, E.G. AN OFFEROR MUST ACCESS AN NIH COMPUTER ROOM FLOOR PLAN. If this paragraph is not applicable to the solicitation, delete it in its entirety.

Make sure to appropriately designate the subparagraph below.

k. Prospective Offeror Non-Disclosure Agreement

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

NOTE: Provide a description of the sensitive Federal Information and select the appropriate Position Sensitivity Designation below.

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

[ ] Level 6: Public Trust - High Risk
[ ] Level 5: Public Trust - Moderate Risk

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

(a) Submit a written request to the Contracting Officer identified in the solicitation;
(b) Complete and submit the "Prospective Offeror Non-Disclosure Agreement" (http://nitaac.nih.gov/downloads/iw2/Prospective_Offeror_Non-Disclosure.doc); and
(c) 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 Federal 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.

l. 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/policies/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/
(4) NIST Special Publication 800-16, Information Technology Security Training Requirements: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
Appendix A-D: http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf

(5) NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

(6) NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

(7) NIST SP 800-53, Revision 1, Recommended Security Controls for Federal Information Systems: http://www.csrc.nist.gov/publications/drafts/800-53-rev1-ipd-clean.pdf

(8) NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume I: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf;
Volume II, Appendices to Guide For Mapping Types of Information and Information Systems To Security Categories, Appendix C at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf and Appendix D at: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf.

(9) NIST SP 800-64, Security Considerations in the Information System Development Life Cycle: http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

(10) FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

(11) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

2. Confidential Treatment of Sensitive Information

DHHS customers include this section if the contractor will have access to sensitive information/data during the performance of the task order that needs to be handled confidentially by the contractor, but including the clause at HHSAR352.224-70, Confidentiality of Information, would be inappropriate. IF THIS IS NOT APPLICABLE TO THE ORDER, DELETE THIS SECTION.

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

3. Certifications

Certifications of the DO and quotation are required if the contractor/subcontractor will (1) develop, (2) have the ability to access, or (3) host and/or maintain a federal automated information system.

The certification in Section 3.1 is to be completed prior to requesting quotations, and the certification in Section 3.2 is to be completed after receipt of quotations and prior to award.

3.1 Request for Quotation (RFQ) Certification

Delivery Order Tracking Number: _____

We certify that the referenced RFQ specifies appropriate security requirements necessary to adequately protect the Government's interests in compliance with all Federal and DHHS security requirements as prescribed by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the DHHS Information Security Program Policy. If this requirement has been initiated by or for another Federal Agency, the security requirements applicable for that Agency are also specified within the referenced delivery order.

The security requirements are set forth in such a manner that all prospective contractors can readily understand what is required.

_____

Project Officer Date

_____

Project Officer's typed name

_____

Information Systems Security Officer Date

_____

Information Systems Security Officer's typed name

3.2 Pre-Award Certification

Delivery Order Tracking Number: _____

We certify that the quotation submitted by _____, dated _____, specifies appropriate security requirements necessary to comply with Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the *DHHS Information Security Program Policy*. If this requirement has been initiated by or for another Federal Agency, the security requirements applicable for that Agency are also specified within the referenced quotation.

_____
Project Officer Date

_____
Project Officer's typed name

_____
Information Systems Security Officer Date

_____
Information Systems Security Officer's typed name