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 (DHHS) customers *and is based on guidance from the DHHS Automated Information Systems Security Program (AISSP) Handbook.* ***Non-DHHS customers should prepare delivery orders in a manner compliant with the security requirements and guidance of their agencies****.*

This Security attachment is to be applied only to DHHS delivery orders involving Information technology (IT) where the contractor will develop or have access to an agency automated information system (AIS) and is subject to the AISSP, or the contractor will have access to sensitive information/data.

The general applicability of this Delivery Order Security Attachment is summarized by ECS III lots in Table 1. Table 2 identifies the delivery-order-specific information required to complete this Security Attachment.

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) 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 ECS III Delivery Orders

Lots	*Applicability of Security Attachment*
1. COTS desktop, laptop and handheld computing devices, workstations, software, and networking equipment	*Not likely, as lots 1 -4 generally do not involve contractor access to an AIS or to sensitive information*
2. Commercial telecommunications equipment items related to telephony	
3. Scientific research workstations, and other electronic devices and systems	
4. Software (including operating systems)	
5. Related warranty and maintenance services	*Likely, as lots 5 and 6 may involve software or system installation, on-site maintenance or support, etc.*
6. Support services that directly support Lots 1-5 products/services	

Table 2. Delivery-Order-Specific Information Required to Complete this Security Attachment

Security Attachment Section	*Information Required*	*Participation Required*
1.0 Information Technology Systems Security	• *Category of safeguarded information* • *Sensitivity level designation for information/data* • *Criticality level designation for operational criticality* • *Overall security level designation* • *Position sensitivity designations (for preparation of quotations)* • *Security training requirements (if other than NIH's Computer Security Awareness Training)*	• *Project Officer*
2.0 Confidential Treatment of Sensitive Information	• *Knowledge of whether the contractor will access sensitive information during the performance of the delivery order*	• *Project Officer*
3.0 Information Technology Systems Security Specifications	• *Security training requirements (as in Section 1.0)* • *Position sensitivity designations (finalized)*	• *Project Officer*
4.0 Certifications	• *Results from the security review of the delivery order and the quotation*	• *Project Officer and Information Systems Security Officer*

1. Information Technology Systems Security

DHHS customers must include this subsection if the delivery order involves, in whole or in part, information technology (IT) where the contractor will develop or have access to an automated information system (AIS), and is subject to the security requirements of the DHHS AISSP.

Note: In addition to guidance from the Project Officer (PO) and Information Systems Security Office (ISSO), Chapters II, VII, and XIV of the DHHS AISSP Handbook should be used as a reference when completing information required for this item. IF THIS IS NOT APPLICABLE TO THE DELIVERY ORDER, DELETE THIS SUBSECTION.

(a) Sensitivity and Security Level Designations.

The delivery order 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:

** ***(NOTE:** See Table 1-Categories of Safeguarded Agency Information on the CIT website for information about each of these categories at* http://irm.cit.nih.gov/security/table1.htm *.)* **

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

(2) Security Level Designations

** ***(NOTE:** For information about determining the security level designations, See Table 2-Security Level Designations for Agency Information, on the CIT website at:* http://irm.cit.nih.gov/security/table2.htm *and Chapter II of the AISSP Handbook at:* http://irm.cit.nih.gov/policy/aissp.html*.)* **

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 __**.

** ***(NOTE:** The overall Security Level designation is the higher of the sensitivity and criticality levels identified above.)* **

(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 delivery order. For quotation preparation purposes, the following designations apply:

** ***(NOTE:** Check all that apply. For information about determining the position sensitivity designations, See Table 3-Position Sensitivity Designations for Individuals Accessing Agency Information, on the CIT website @* http://irm.cit.nih.gov/security/table3.htm *and Chapter VII of the AISSP Handbook at* http://irm.cit.nih.gov/policy/aissp.html*.)* **

[ ] 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.

*** (**NOTE:** The AISSP Handbook in Section XIV.D.4.d states that contractors are to pay the cost of required security background investigations. If this requirement is not applicable to your order, please delete the sentence below. (This requirement is not explicitly included in NIH/NCI contracting forms, which are the source for this DO Security Attachment.) ***

The winning contractor shall pay the cost of required security background investigations for contractor employees.

(b) **Information Technology (IT) System Security Program**

The offeror's quotation must:

(1) Include a detailed outline (commensurate with the size and complexity of the requirements of the delivery order) 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.

(NOTE:** You must fill in the Overall Security Level designation from paragraph (a)(2) above.)

(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.

(**NOTE**: DHHS Operational Divisions other than NIH may replace the reference to NIH Computer Security Awareness Training below with another DHHS security training course as appropriate.)

The successful offeror will be responsible for assuring that each contractor employee has completed the following NIH Computer Security Awareness Training course prior to performing any contract work: http://irtsectraining.nih.gov/. The contractor will be required to maintain a listing of all individuals who have completed this training and submit this listing to the Government.

Additional security training requirements commensurate with the position may be required as defined in OMB Circular A-130 or NIST Special Publication 800-16, "Information Technology Security Training Requirements." These documents provide information about IT security training that may be useful to potential offerors.

*** (**NOTE:** Include below when a prospective offeror will require access to sensitive information in order to prepare a quotation, 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 a quotation.

*** (**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.

*** (**NOTE:** Include below in **ALL** solicitations that include IT System Security requirements. If subparapgraph (d) above is not applicable to your solicitation, change subparagraph designation from (e) to (d) below.) ***

(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://irm.cit.nih.gov/security/secplantemp.doc
(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

2. Confidential Treatment of Sensitive Information

If the contractor will have access to sensitive information/data during the performance of this order that needs to be handled confidentially by the contractor, then select one of the following two alternatives for protecting that information/data:

If the clause at HHSAR 352.224-70, Confidentiality of Information, is appropriate for your order, then state that this clause applies to this order and then delete the remaining content of Section 2 below.

OR

If the clause at HHSAR 352.224-70 is not appropriate for your order, please include Section 2 as it is presently constructed below.

IF NONE OF THE ABOVE APPLIES (THAT IS, THE CONTRACTOR WILL HAVE NO ACCESS TO SENSITIVE INFORMATION/DATA), THEN DELETE SECTION 2.

The Contractor shall guarantee strict confidentiality of the information/data that it is provided by the Government during the performance of the delivery order. The Government has determined that the information/data that the Contractor will be provided during the performance of the delivery 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 delivery order, the Contractor shall obtain a written determination from the Contracting Officer.

3. Information Technology Systems Security Specifications

DHHS customers must include this subsection if the delivery order involves, in whole or in part, IT where the contractor will develop or have access to an AIS, and is subject to the security requirements of the DHHS AISSP.
Note: For more information about IT Security requirements see Chapters VII and XIV of the DHHS AISSP Handbook, including Exhibits VII-B, XIV-C and XIV-D. IF THIS IS NOT APPLICABLE TO THE DELIVERY ORDER, DELETE THIS SUBSECTION.

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 delivery order. 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 DELIVERY ORDER. 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.

Procedural guidance for compliance with the following requirements can be found at the following website: http://virtual.nci.nih.gov/security/policy/aissp/contractor/.

a. Required IT Systems Security Training

*** (NOTE: DHHS Operational Divisions other than NIH may replace the reference to NIH Computer Security Awareness Training below with another DHHS security training course if appropriate.) ***

The contractor shall assure that each employee has completed the NIH Computer Security Awareness Training (http://irtsectraining.nih.gov/) prior to performing any work under this delivery order.

*** (NOTE: 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 paragraph below provides specific instructions on its submission.) ***

The contractor shall maintain a listing by name and title of each individual working under this delivery order 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 shall be delivered to the Project Officer within 10 calendar days after contractor receipt of the delivery order. Any revisions to this listing as a result of staffing changes shall be submitted with 10 calendar days after each staffing change.]

*** (NOTE: If the Government will require contractor 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.) ***

As indicated in OMB Circular A-130 and/or NIST Special Publication 800-16, "Information Technology Security Training Requirements," contractor staff shall complete the following additional training prior to performing any work under this delivery order:

[List the required training courses here.]

b. Position Sensitivity Designations

(1) The Government has determined that the following position sensitivity designations and associated clearance and investigation requirements apply under this delivery order:

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

Select only the applicable designation(s). Delete those that do not apply. Table 3 - Position Sensitivity Designations for Individuals Accessing Agency Information, on the CIT website at http://irm.cit.nih.gov/security/table3.htm and Chapter VII of the DHHS AISSP Handbook at http://irm.cit.nih.gov/policy/aissp.html include information about Position Sensitivity Designations.

*If more than one of the below designations apply to the delivery order, the CO, PO & ISSO may wish to consider whether there is a need to identify specific Contractor Position Titles with the applicable sensitivity designations. If there is, make sure to list them here in this Article.) ***

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.)* **

(2) The contractor shall submit a roster, by name, position and responsibility, of all IT staff working under the delivery order. The roster shall be submitted to the Project Officer, with a copy to the Contracting Officer, within 14 days of the effective date of the delivery order. The Project Officer shall notify the contractor of the appropriate level of suitability investigations to be performed. An electronic template, entitled "Roster of Employees Requiring Suitability Investigations," is available for use at http://virtual.nci.nih.gov/security/policy/aissp/contractor/forms/Suitability-roster.xls.

Upon receipt of the Government's notification of applicable Suitability Investigation required, the contractor shall complete and submit the required forms within 30 days of the notification. Additional submission instructions can be found at: http://virtual.nci.nih.gov/security/policy/aissp/contractor/

Contractor employees who have had a background investigation conducted by the U.S. Office of Personnel Management (OPM) within the last five years may only require an updated or upgraded investigation.

(3) 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 delivery order.

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.

***(NOTE: The Project Officer will submit requests for investigations and verifications of completed investigations. For NIH customers, requests are submitted to the cognizant Division of Human Resource Operation (DHRO) branch, which will coordinate investigations with the NIH Personnel Security Program Manager (NIH/OM/HR/DERT, EPS 100, 594-1456), and will inform the Project Officer when investigations have been completed. Other DHHS Operational Divisions would follow a similar process as prescribed by their ISSO.) ***

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 delivery order.

4. Certifications

Certifications of the DO and quotation are required if the delivery order involves IT where the contractor will develop or have access to an agency AIS, and is subject to AISSP security requirements. IF THIS IS NOT APPLICABLE TO THE DELIVERY ORDER, DELETE THIS SUBSECTION.

The certification in Section 4.1 is to be completed prior to requesting quotations, and the certification in Section 4.2 is to be completed after receipt of quotations and prior to award.

4.1 Solicitation Certification

We certify that the referenced delivery order 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 Automated Information Systems Security Program (AISSP) Handbook. 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

4.2 Pre-Award Certification

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 Automated Information Systems Security Program (AISSP) Handbook*. 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