H.13 INFORMATION SECURITY (Revision 2)

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

The provisions below are applicable to Department of Health and Human Services (DHHS) task 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 is subject to the security requirements of the DHHS Information Security Program Policy. When applicable, the task order SOW will include the provisions below completed with task-order-specific information.

For more information about Information Security see:
DHHS Information Security Program Policy at:
(http://www.hhs.gov/read/irmpolicy/FINALHHSInformationSecurityProgramP.doc)
and
DHHS Information Security Program Handbook at:
(http://intranet.hhs.gov/infosec/docs/policies_guides/ISPPH/PG_IT_Security_Handbook_12012005.pdf).

The Statement of Work (SOW) requires the contractor to develop or access Federal automated information systems; therefore, the contractor shall comply with the "DHHS Information Security Program Policy" (http://www.hhs.gov/read/irmpolicy/FINALHHSInformationSecurityProgramP.doc) as set forth below. The contractor shall include this provision in any subcontract awarded under this contract.

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

(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).

[ ] 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).

[ ] 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 and responsibility, of all IT staff working under the contract. 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 contract. The Contracting Officer shall notify the contractor of the appropriate level of suitability investigations to be performed. Any revisions to the roster as a result of staffing changes shall be submitted within fifteen (15) calendar days of the change. 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 Investigation 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 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 shall comply with the DHHS criteria for the assigned position sensitivity designations prior to performing any work under this contract. The following exceptions apply:

Levels 5 and 1: Contractor 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 (2) above.

Level 6: In special circumstances the Project Officer may request a waiver of the preappointment investigation. If the waiver is granted, the Project Officer will provide written authorization for the contractor employee to work under the contract.

d. Systems Security Plan

The appropriate sentence within the brackets below would be selected during task order creation.

The contractor shall protect Federal automated information systems that are developed or accessed by the contractor. [System security shall be accomplished in accordance with the contractor's System Security Plan dated _____. ***/OR*** The Systems Security Plan (SSP) that the contractor submitted with its offer shall be finalized in coordination with the Project Officer no later than 90 calendar days after contract award. The plan must:]

The appropriate subparagraph (1) below would be selected during task order creation. If the subparagraph is not applicable, it would be deleted entirely.

(1) Include a detailed plan of present and proposed systems security programs commensurate with the size and complexity of the requirements of the Statement of Work. The contractor shall use the **NIH Systems Security Plan Template** (detailed) at http://irm.cit.nih.gov/security/secplantemp.doc or **NIH Systems Security Plan Outline** (outline only) at http://irm.cit.nih.gov/nihsecurity/Security_Plan_Outline.doc.

or

(1) Include a plan of present and proposed systems security programs commensurate with the size and complexity of the requirements of the Statement of Work. The minimum areas to be addressed include, but are not limited to administrative, technical, and physical security as follows:

(i) Security Awareness Training
(ii) Logical Access Control
- -Network (ex: firewall)
- -System (ex: network OS, tcp wrappers, SSH)
- -Application (ex: S-LDAP, SSL)
- -Remote Access (ex: VPN)
- -Monitoring and support (ex: IDS, pager, NOC)

(iii) Protection against data loss
- -OS security (ex: patch management, configuration)
- -Application security (ex: patch management)
- -Database security
- -Back-up and recovery
- -Fault tolerance, high availability

(iv) Malicious Code Protection (ex: Antivirus, filtering of e-mail attachments, etc.)
(v) Physical Security
- -Access control (ex: locks, guards)
- -Power conditioning and/or UPS
- -Air conditioning
- -Fire protection

Include an acknowledgment of its understanding of the security requirements.

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

e. Rules of Behavior

The contractor shall comply with the DHHS Rules of Behavior set forth in **DHHS Information Security Program Policy Handbook, Appendix G** at:
http://intranet.hhs.gov/infosec/docs/policies_guides/ISPPH/PG_IT_Security_Handbook_12012005.pdf; and

the **NIH Information Technology General Rules of Behavior** at:
http://irm.cit.nih.gov/security/nihitrob.html.

f. Information Security Training

Each contractor employee shall complete the NIH Computer Security Awareness Training (http://irtsectraining.nih.gov/) prior to performing any contract work, and on an annual basis thereafter, during the period of performance of this contract.

The contractor shall maintain a listing by name and title of each individual working under this contract that has completed the NIH required training. Any additional security training completed by contractor 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.]

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

Required training courses, if any, would be listed here.

g. Personnel Security Responsibilities

The contractor shall perform and document the actions identified in the "Employee Separation Checklist", attached and made a part of this contract, when a contractor 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 Departmental Information Systems and Data

(1) Contractor Agreement

The Contractor shall not release, publish, or disclose 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 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 Department information under this contract shall complete 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.

i. References

(1) DHHS Information Security Program Policy:
(http://www.hhs.gov/read/irmpolicy/FINALHHSInformationSecurityProgramP.doc
(2) DHHS Personnel Security/Suitability Handbook:
http://www.hhs.gov/ohr/manual/pssh.pdf
(3) 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
(4) NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems:
http://csrc.nist.gov/publications/nistpubs/index.html
(5) 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

(6) NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II:
http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf

(7) 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

(8) NIH Computer Security Awareness Training Course:
http://irtsectraining.nih.gov/

(9) Roster of Employees Requiring Suitability Investigations:
http://ais.nci.nih.gov/forms/Suitability-roster.xls

(10) NCI Information Technology Security Policies, Background Investigation Process:
http://ais.nci.nih.gov/

(11) NIH Systems Security Plan Template (detailed):
http://irm.cit.nih.gov/security/secplantemp.doc

(12) NIH Systems Security Plan Outline (outline only):
http://irm.cit.nih.gov/nihsecurity/Security_Plan_Outline.doc

(13) NIH Information Technology General Rules of Behavior:
http://irm.cit.nih.gov/security/nihitrob.html

(14) Commitment To Protect Non-Public Information - Contractor Agreement:
http://irm.cit.nih.gov/security/Nondisclosure.pdf

(15) Employee Separation Checklist:
http://rcb.cancer.gov/rcb-internet.nci.nih.gov/forms/Emp-sep-checklist.pdf

(16) OMB A-130, Appendix III:
http://csrc.nist.gov/policies/appendix_iii.pdf

H.29 Contract Earned Value Management Requirements

Task orders under this contract may be subject to Earned Value Management (EVM) requirements, and thereby contractors may be required to implement an Earned Value Management System (EVMS) in the performance of a task order. An EVMS is defined in FAR 2.101(b) of the proposed rule on Earned Value Management, case no. 2004-019, as follows.

> *Earned value management system* means a project management tool that effectively integrates the project scope of work with cost, schedule and performance elements for optimum project planning and control. The qualities and operating characteristics of earned value management systems are described in American National Standards Institute (ANSI)/Electronics Industries Alliance (EIA) Standard–748, Earned Value Management systems. (See OMB Circular A–11, Part 7.)

The ordering (customer) agency's policies will be the relevant authority in determining which EVMS requirements apply for individual task order awards under this contract. Task orders are subject to EVMS requirements commensurate with the customer agency's policy for the information technology Development, Modernization, or Enhancement investment for which the order is being placed.

Customers will ensure that task order solicitations are in compliance with proposed FAR Subpart 34.X "Earned Value Management Systems" of the FAR proposed rule on Earned Value Management. The following proposed clause (FAR 52.234-X3 Earned Value Management System) will be used in task orders as appropriate.

> (a) In the performance of this contract the Contractor shall use an earned value management system (EVMS) to manage the contract that at the time of contract award has been recognized by the cognizant Administrative Contracting Officer (ACO) or a Federal department or agency as compliant with the guidelines in ANSI/EIA Standard-748-98 (current version at time of award) and the Contractor will submit reports in accordance with the requirements of this contract.
>
> (b) If, at the time of award, the Contractor's EVMS has not been recognized by the cognizant ACO or a Federal department or agency as complying with EVMS guidelines (or the Contractor does not have an existing cost/schedule control system that is compliant with the guidelines in ANSI/EIA Standard-748-98 (current version at time of award)), the Contractor shall apply the system to the contract and shall be prepared to demonstrate to the ACO that the EVMS complies with the EVMS guidelines referenced in paragraph (a) of this clause.
>
> (c) Agencies may conduct Integrated Baseline Reviews (IBR). If a pre-award IBR has not been conducted, such a review shall be scheduled as early as practicable after contract award, but not later than 180 days after award. The Contracting Officer may also require an IBR at (1) exercise of significant options or (2) incorporation of major modifications. Such reviews will normally be scheduled before award of the contract action.
>
> (d) Unless a waiver is granted by the ACO or Federal department or agency, Contractor proposed EVMS changes require approval of the ACO or Federal department or agency, prior to implementation. The ACO or Federal department or agency, shall advise the Contractor of the acceptability of such changes within 30 calendar days after receipt of the notice of proposed changes from the Contractor. If the advance approval requirements are waived by the ACO or Federal department or agency, the Contractor shall disclose EVMS changes to the ACO or Federal department or agency at least 14 calendar days prior to the effective date of implementation.

(e) The Contractor agrees to provide access to all pertinent records and data requested by the Contracting Officer or a duly authorized representative. Access is to permit Government surveillance to ensure that the EVMS conforms, and continues to conform, with the performance criteria referenced in paragraph (a) of this clause.

(f) The Contractor shall require the subcontractors specified below to comply with the requirements of this clause: [Insert list of applicable subcontractors.]

(End of clause)