H.7 Information Security (Revision 2)

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

The provisions below are applicable to Department of Health and Human Services (HHS) task orders for which contractor/subcontractor personnel will (1) develop, (2) have the ability to access, or (3) host and/or maintain a Federal information system(s).

For more information, see HHS Information Security Program Policy at:
http://intranet.hhs.gov/infosec/docs/policies_guides/ISPP/Information_Security_Program_Policy_07192005.doc*;*
and the HHS Information Security Program Handbook at:
http://intranet.hhs.gov/infosec/docs/policies_guides/ISPPH/PG_IT_Security_Handbook_12012005.doc*.*

When applicable, the task order SOW will include the provisions below completed with task-order-specific information and possibly tailored to specific HHS component needs.

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/policies/FISMA-final.pdf.

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 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 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 contract.

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 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 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.]

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

The required training courses would be specified in the SOW.

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 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 (http://nitaac.nih.gov/downloads/iw2/Contractor_Employee_Non-Disclosure.doc). 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. NIST SP 800-26 Self-Assessment Questionnaire

The contractor shall annually update and re-submit its Self-Assessment Questionnaire required by NIST Draft SP 800-26, Revision 1, Guide for Information Security Program Assessments and System Reporting Form (http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.pdf - See Appendix B for format). NIST 800-26 assesses information security assurance of the offeror's internal systems security. This assessment is based on the Federal IT Security Assessment Framework and Draft NIST SP 800-53, Revision 1, Recommended Security Controls for Federal Information Systems, at: (http://www.csrc.nist.gov/publications/drafts/800-53-rev1-ipd-clean.pdf).

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 due date for the annual update below would be specified in the SOW.

The annual update shall be submitted to the Project Officer, with a copy to the Contracting Officer.

The provision below will be included in an HHS SOW when:

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

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 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.

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.

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, Revision 1, Computer Security: http://csrc.nist.gov/publications/drafts/Draft-sp800-26Rev1.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

H.34 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 FAR Subpart 34.2 "Earned Value Management Sys tem." This subpart of the FAR requires the contracting officer to insert clauses substantially the same as the following:

- In solicitations for contracts that require the contractor to use an Earned Value Management System (EVMS) and for which the Government requires an Integrated Baseline Review (IBR) prior to award, use the following provision at 52.234-2:

> NOTICE OF EARNED VALUE MANAGEMENT SYSTEM - PRE-AWARD IBR (JULY 2006)
>
> (a) The offeror shall provide documentation that the Cognizant Federal Agency has determined that the proposed earned value management system (EVMS) complies with the EVMS guidelines in ANSI/EIA Standard - 748 (current version at time of solicitation).
> (b) If the offeror proposes to use a system that has not been determined to be in compliance with the requirements of paragraph (a) of this provision, the offeror shall submit a comprehensive plan for compliance with the EVMS guidelines.
> (1) The plan shall—
> (i) Describe the EVMS the offeror intends to use in performance of the contracts;
> (ii) Distinguish between the offeror's existing management system and modifications proposed to meet the guidelines;
> (iii) Describe the management system and its application in terms of the EVMS guidelines;
> (iv) Describe the proposed procedure for administration of the guidelines, as applied to subcontractors; and
> (v) Provide documentation describing the process and results of any third-party or self-evaluation of the system's compliance with the EVMS guidelines.

(2) The offeror shall provide information and assistance as required by the Contracting Officer to support review of the plan.

(3) The Government will review and approve the offeror's plan for an EVMS before contract award.

(4) The offeror's EVMS plan must provide milestones that indicate when the offeror anticipates that the EVM system will be compliant with the ANSI/EIA Standard - 748 guidelines.

(c) Offerors shall identify the major subcontractors, or major subcontracted effort if major subcontractors have not been selected subject to the guidelines. The prime Contractor and the Government shall agree to subcontractors selected for application of the EVMS guidelines.

(d) The Government will conduct an Integrated Baseline Review (IBR), as designated by the agency, prior to contract award. The objective of the IBR is for the Government and the Contractor to jointly assess technical areas, such as the Contractor's planning, to ensure complete coverage of the contract requirements, logical scheduling of the work activities, adequate resources, methodologies for earned value (budgeted cost for work performed (BCWP)), and identification of inherent risks.

(End of provision)

- In solicitations for contracts that require the contractor to use an Earned Value Management System (EVMS) and for which the Government requires an Integrated Baseline Review (IBR) after contract award, use the following provision at 52.234-3:

NOTICE OF EARNED VALUE MANAGEMENT SYSTEM - POST AWARD IBR (JULY 2006)

(a) The offeror shall provide documentation that the Cognizant Federal Agency has determined that the proposed earned value management system (EVMS) complies with the EVMS guidelines in ANSI/EIA Standard - 748 (current version at time of solicitation).

(b) If the offeror proposes to use a system that has not been determined to be in compliance with the requirements of paragraph (a) of this provision, the offeror shall submit a comprehensive plan for compliance with the EVMS guidelines.

(1) The plan shall—

(i) Describe the EVMS the offeror intends to use in performance of the contracts;

(ii) Distinguish between the offeror's existing management system and modifications proposed to meet the guidelines;

(iii) Describe the management system and its application in terms of the EVMS guidelines;

(iv) Describe the proposed procedure for administration of the guidelines, as applied to subcontractors; and

(v) Provide documentation describing the process and results of any third-party or self-evaluation of the system's compliance with the EVMS guidelines.

(2) The offeror shall provide information and assistance as required by the Contracting Officer to support review of the plan.

(3) The Government will review and approve the offeror's plan for an EVMS before contract award.

(4) The offeror's EVMS plan must provide milestones that indicate when the offeror anticipates that the EVM system will be compliant with the ANSI/EIA Standard -748 guidelines.

(c) Offerors shall identify the major subcontractors, or major subcontracted effort if major subcontractors have not been selected, planned for application of the guidelines. The prime Contractor and the Government shall agree to subcontractors selected for application of the EVMS guidelines.

(End of provision)

- In solicitations and contracts that require a contractor to use an EVMS, use the following provision at 52.234-4:

EARNED VALUE MANAGEMENT SYSTEM (JULY 2006)

(a) The Contractor shall use an earned value management system (EVMS) that has been determined by the Cognizant Federal Agency (CFA) to be compliant with the guidelines in ANSI/EIA Standard - 748 (current version at the time of award) to manage this contract. If the Contractor's current EVMS has not been determined compliant at the time of award, see paragraph (b) of this clause. The Contractor shall submit reports in accordance with the requirements of this contract.

(b) If, at the time of award, the Contractor's EVM System has not been determined by the CFA 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 (current version at time of award), the Contractor shall—

(1) Apply the current system to the contract; and

(2) Take necessary actions to meet the milestones in the Contractor's EVMS plan approved by the Contracting Officer.

(c) The Government will conduct an Integrated Baseline Review (IBR). If a pre-award IBR has not been conducted, a post award IBR shall be conducted as early as practicable after contract award.

(d) The Contracting Officer may require an IBR at—

(1) Exercise of significant options; or

(2) Incorporation of major modifications.

(e) Unless a waiver is granted by the CFA, Contractor proposed EVMS changes require approval of the CFA prior to implementation. The CFA will 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 CFA, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or a duly authorized representative as necessary 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.

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

_____

_____

_____

_____

(End of clause)