# CIO-SP2*i* – NITAAC Statement of Work (SOW)

**Task Order Title**

**As of mm/dd/yy**

**Agency**

*Note: Guidance is presented in italics with paragraph borders, while example content is presented in normal font.* ***Please delete all guidance when finalizing the SOW.***

*The SOW must have an "as of date." If the SOW is revised or corrected during the pre-award phase, each revision must have a new date with changes marked by revision bars. When a SOW is revised for task order modification (after award) it must be given a new As of date. SOW's must be page numbered.*

*Customers submit electronic copies of the Task Order Requirements Package (TORP) and attachments via e-mail or compact disk. Electronic documents may be in MS Word or WordPerfect; and MS Excel or Lotus 123. Signed documents must be submitted in hardcopy via fax or U.S. mail.*

## 1. Task Order Title

*Include a short title of services or a general description of items to be acquired. This title should be unique and descriptive, and should be used consistently thought the task order process.*

## 2. Background

*Justify this effort in relationship to the customers' agency mission. List other historical or parallel efforts such as other agency activities and/or industry efforts that provide additional information related to this SOW.*

## 3. Objectives

*Provide a concise overview of the customer's goals and expectations as a result of this task order.*

## 4. Scope

*Describe the general scope of work. The SOW must be performance-based in accordance with FAR 37.6, unless a rationale is provided for not using performance based contracting methods. Each SOW must contain Contract Level and Task Order (TO) Management. Identify each CIO-SP2i Task Order work category required to ensure that your tasks are within contract scope (mandatory).*

*For example:*

*CIO-SP2i Task Area 1. Chief Information Officer (CIO) Support*
*CIO-SP2i Task Area 2. Outsourcing*
*CIO-SP2i Task Area 3. IT Operations and Maintenance*
*CIO-SP2i Task Area 4. Integration Services*
*CIO-SP2i Task Area 5. Critical Infrastructure Protection and Information Assurance*
*CIO-SP2i Task Area 6. Digital Government*
*CIO-SP2i Task Area 7. Enterprise Resource Planning*
*CIO-SP2i Task Area 8. Clinical Support, Research, and Studies*
*CIO-SP2i Task Area 9. Software Development*

## 5. Specific Tasks

*Provide a performance-based narrative of the specific tasks and/or products that make up the SOW. Number the tasks sequentially, e.g. Task 1 and narrative, Task 2 and narrative, etc. Task 1 for each*

*SOW must be for Contract-Level and Task Order (TO) Management, and must contain two subtasks at a minimum, with the following narratives:*

*Task 1 - Contract-Level and Task Order (TO) Management (mandatory)*
*Subtask 1 - Contract Level Program Management*
*Subtask 2 - Task Order Management*

## 5.1 Task 1 - Contract-Level and Task Order (TO) Management

### 5.1.1 Subtask 1 – Contract-Level Program Management

*Provide the technical and functional activities at the contract level needed for program management of this SOW. Including productivity and management methods such as Quality Assurance, Configuration, Work Breakdown Structure, and Human Engineering at the Contract level. Provide the centralized administrative, clerical, documentation and other related functions.*

### 5.1.2 Subtask 2 - Task Order Management

*Prepare a Task Order Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.*

#### 5.1.2.1 Earned Value Management System

*All task orders on this contract are required to meet appropriate Earned Value Management System (EVMS) requirements. Orders from agencies other than Health and Human Services (HHS) are required to meet their agency's EVMS requirements, and by customer certification in the TORP letter that they are doing so, are not subject to the HHS EVMS requirements.*

*HHS task orders must adhere to the HHS EVMS policy. Per HHS policy, EVMS requirements implemented for task orders on the CIO-SP2i contract are determined by the planned Development, Modernization, or Enhancement (DME) expenditures. If the task order supports an agency's IT investment (as indicated by inclusion of task order funds on the Agency's Exhibit 53, or in an Exhibit 300 for that investment), the relevant dollar amount for the task order is the total planned DME expenditure for that investment; if the task order is not part of a larger IT investment, then the relevant dollar amount for the task order is the total DME value of the task order only. The HHS EVMS tiers, and the associated requirements, are defined as follows:*

*(a) Task Orders for investments that meet or exceed the HHS Tier I threshold of $10,000,000 of planned DME expenditures must require either:*
- *the use of an EVMS that has been determined by the Cognizant Federal Agency (CFA) to be compliant with the guidelines in American Nation Standards Institute (ANSI)/ Electronic Industries Alliance (ANS/IEIA) Standard-748 (current version at time of award); or*
- *the use of an EVMS that can be shown to be compliant with the standard.*

*(b) Task Orders for investments that meet the HHS Tier II definition of equal to or greater than $1,000,000 and less than $10,000,000 of planned DME expenditures must require that a subset of the ANSI/EIA Standard-748 be met by the contractor's EVMS. See Attachment 2 of the HHS OCIO IT Earned Value Management Processes and Procedures, December 30, 2005, (http://www.hhs.gov/ocio/policy/policydocs/20070001.doc). Additionally, an Integrated Baseline Review is optional, depending upon the project manager's risk-based judgment.*

*(c) Task Orders for investments that meet the HHS Tier III definition of under $1,000,000 of planned DME expenditures must require the use of EVM principles appropriate to the level of investment and complexity of the TO.*

*All customers will ensure that task order solicitations are in compliance with FAR Subpart 34.2 "Earned Value Management System." This subpart of the FAR requires the contracting officer to insert provisions and 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 provision at FAR 52.234-2.*
- *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 provision at FAR 52.234-3.*
- *In solicitations and contracts that require a contractor to use an EVMS, use the clause at FAR 52.234-4.*

ALL CUSTOMERS MAY USE THE PROSE PROVIDED BELOW IF SUITED TO YOUR TASK ORDER (THE LANGUAGE IS DRAWN FROM FAR 52.234-4, EARNED VALUE MANAGEMENT SYSTEM AND FROM HHS POLICY DOCUMENTATION).

IF EVMS REQUIREMENTS DO NOT APPLY TO YOUR TASK ORDER, DELETE THIS SUBSECTION.

The following Earned Value Management System (EVMS) requirements apply to this task order:

(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 all subcontractors working on this task order to comply with the EVMS requirements of this statement of work.

The following FAR provisions, where checked, also apply to this task order:

*All customers check one, as appropriate:*

[ ] FAR 52.234-2, NOTICE OF EARNED VALUE MANAGEMENT SYSTEM - PRE-AWARD IBR (JULY 2006)

[ ] FAR 52.234-3, NOTICE OF EARNED VALUE MANAGEMENT SYSTEM - POST AWARD IBR (JULY 2006)

The contractor shall implement an EVMS consistent with the following guidance, where checked:

*HHS customers check one, as appropriate. Other customers should replace this requirement with their own agency's requirements.*

[ ] HHS EMV Tier I requirements as defined in Attachment 1of the HHS OCIO IT Earned Value Management Processes and Procedures, December 30, 2005.

[ ] HHS EVM Tier II requirements as defined in Attachment 2 of the HHS OCIO IT Earned Value Management Processes and Procedures, December 30, 2005.

[ ] HHS EVM Tier III requirements--the Contractor shall apply EMVS principles for tracking investment cost, schedule, and performance.

### 5.1.3 Subtask 3 - In progress Review Support

*Provide a monthly status report monitoring the quality assurance, configuration management, and security management applied to the task order (as appropriate to the specific nature of the SOW).*

### 5.2 Task 2 - Example: Integration Services

***The task title (corresponding to the CIO-SP2i Task Order work Category) is mandatory**. Text in this section precisely describes the work to be performed and/or the products requested. The requirements must be defined sufficiently for the contractor to submit a realistic proposal and the Government to negotiate a meaningful price.*

*EXAMPLE:*
*5.2.1 Subtask 1 - Requirements Definition*
*5.2.2 Subtask 2 - State-of-the-Art-Review*
*5.2.3 Subtask 3 - Design Prototype*
*5. 2.4 Subtask 4 - Integrate Prototype*
*5.2.5 Subtask 5 - Document Prototype*
*5.2.6 Subtask 6 - Train Staff to Use Program*
*5.2.7 Subtask 7 - Participate in Joint Prototype Evaluation*
*5.2.8 Subtask 8 - Document Lessons Learned from Prototype Evaluation*
*5.2.9 Subtask 8 - Establish Baseline Hardware and Software Configuration*

## 6. Contract Type

*State the contract type of contemplated—Firm Fixed Price (FFP), Time and Materials (T&M), Cost Plus Fixed Fee (CPFF), Cost Plus Award Fee (CPAF), or Cost Sharing (CS).*

## 7. Place of Performance

*Specify whether work is to be performed at the contractor site or at a Government Site.*

## 8. Period of Performance

*State the total number of calendar days after the Task Order award necessary for performance. State, if the task order is to be awarded with a base period and options. If the task order is to be awarded and funded incrementally state the base obligation period and incremental funding periods.*

## 9. Deliverables/Delivery Schedule

*Describe precisely the items to be delivered, both during the period of performance and at completion of the task order. Describe the schedule either in terms of calendar days from the date of Task Order award or in calendar days when other projects or program elements are dependent on the delivery (e.g., 10 calendar days after draft plan is approved). The table below provides an example list of deliverables.*

| *SOW TASK #* | *DELIVERABLE TITLE* | *#CALENDAR DAYS AFTER TO AWARD* |
|---|---|---|
| *1* | *Task Order Management Plan* | *Draft - 15, Final - 30* |
| 2 | *Status Report* | *Monthly, on 10th calendar day* |
| *(Continue as needed to document all deliverables)* | | |

## 10. Security

*THE FOLLOWING MATERIAL IS 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://www.hhs.gov/ocio/policy/2004-0002.001.html#intro.

*Non-HHS customers should craft this section to be compliant with the security requirements and guidance of their agencies.*

*Throughout this provision, HHS customers must insert security Information requirements relevant to their task order. Your Project Officer (PO) and your Information Systems Security Officer (ISSO) will assist you in identifying this information.*

*The material in this section set off in boxed italics is guidance information and should be deleted when this section is used for a specific task order. In addition, delete any part of the text that does not apply or that the guidance information instructs you to delete.*

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

This 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 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-rev1/SP800-60_Vol2-Rev1.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-rev1/SP800-60_Vol2-Rev1.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-rev1/SP800-60_Vol2-Rev1.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 to 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 statement of work 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 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. 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.

f. Personnel Security Responsibilities

**Contractor Notification of New and Departing Employees Requiring Background Investigations**

1. The Contractor shall notify the Contracting Officer, the Project Officer, and the Security Investigation Reviewer **within five working days** before a new employee assumes a position that requires a suitability determination or when an employee with a security clearance stops working under the contract. The Government will initiate a background investigation on new employees requiring security clearances and will stop pending background investigations for employees that no longer work under the contract.
2. New employees: Provide the name, position title, e-mail address, and phone number of the new employee. Provide the name, position title and suitability level held by the former incumbent. If the employee is filling a new position, provide a description of the position and the Government will determine the appropriate security level.
3. Departing employees:
   - Provide the name, position title, and security clearance level held by or pending for the individual.
   - Perform and document the actions identified in the "Employee Separation Checklist" (http://nitaac.nih.gov/downloads/ciosp2/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.

g. 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 task order shall complete the Commitment to Protect Non-Public Information - Contractor Agreement (http://nitaac.nih.gov/downloads/ciosp2/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.

*INCLUDE SECTION h, BELOW, WHEN THE SOW 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**.

h. 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 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.

*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 i, BELOW, 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.*

*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.*

i. 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 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.

*INCLUDE SECTION j, 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.*

j. 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/ciosp2/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.

k. 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/drivers/documents/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 800-53, Revision 1, Recommended Security Controls for Federal Information Systems: http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf.
(7) 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-rev1/SP800-60_Vol1-Rev1.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-rev1/SP800-60_Vol2-Rev1.pdf and Appendix D at: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.
(8) NIST SP 800-64, Security Considerations in the Information System Development Life Cycle: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
(9) 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
(10) FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems:

http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

### 10.1 Confidential Treatment of Sensitive Information

*DHHS customers must include this subsection 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 TASK ORDER, DELETE THIS SUBSECTION.*

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.

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; and
(b) Receive written approval from the Contracting Officer.

### 10.2 System Configuration Security

DHHS customers must include this subsection if the services required include configuration of any systems or applications for which there exist Agency Configuration Standards or NIST Security Checklist Standards. IF THIS IS NOT APPLICABLE TO THE TASK ORDER, DELETE THIS SUBSECTION.

If the services required include configuration of any systems or applications for which there exist Agency Configuration Standards or NIST Security Checklist Standards, then the SOW must require that these configurations conform to the Agency or NIST standard.

## 11. Government Furnished Equipment (GFE)/ Government Furnished Information (GFI)

*Identify any GFE and/or GFI and any limitations that will be provided to the contractor.*

## 12. Packaging, Packing, and Shipping Instructions

*At a minimum, the SOW should state the following.*

The contractor shall ensure that all items are preserved, packaged, packed and marked in accordance with best commercial practices to meet the packing requirements of the carrier and to ensure safe and timely delivery at the intended destination. All data and correspondence submitted shall reference:

1. The CIO-SP2*i* Task Order Authorization Number
2. The NITAAC Tracking Number
3. The government end user agency
4. The name of the COTR

Containers shall be clearly marked as follows:

1. Name of contractor
2. The CIO-SP2*i* Task Order Authorization Number
3. The NITAAC Tracking Number
4. Description of items contained therein
5. Consignee(s) name and address

*State special requirements if they exceed these requirements.*

## 13. Inspection and Acceptance Criteria

*At a minimum, the SOW must specify a Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery. State special requirements if they exceed the contract requirement. A Quality Assurance Surveillance Plan (QASP) must be included here, in Section 15, or attached as a separate document (see Section 15). State here if the Government is requiring offerors to submit a proposed QASP.*

## 14. Accounting and Appropriation Data

*Specify customer's standard funding documentation (e.g., Common Accounting Number). A statement must be made that funds are available for this task order or will become available prior to award. If funds are to be provided from the next fiscal year a statement that the task order is subject to availability of funds must be made in the task order request.*

## 15. Other Pertinent Information or Special Considerations

*Include any special considerations or unique requirements necessary to accomplish the task order (e.g., specialized experience with UNIX etc.) and/or any additional information that will be helpful in determining reasonable approaches and cost estimates for the task order. As appropriate, this section needs to contain:*

1. *Identification of possible follow-on work that may result from completion of this task order.*
2. *Identification of potential Conflicts of Interest (COI's) that may influence which contractors should be awarded the task order. (See Far 9.501)*
3. *Contractor Travel - Describe any local or long distance travel the contractor will have to perform to execute the task order. Identify the to/from locations of the travel, numbers and duration of the trip.*
4. *Architectural Standards - Describe requirements for compliance with agency architectural standards.*
5. *If a fixed price task order is contemplated, specify procedures for reduction of fees or for reductions in the price of the task order when services are not performed or do not meet task order requirements.*
6. *Use measurable performance standards (i.e., in terms of quality, timeliness, quantity, etc.) and include performance incentives where appropriate (per FAR Subpart 37.6 or FAR Part 46). All Task Orders must have a Quality Assurance Surveillance Plan (QASP) submitted with this SOW form. The QASP may be integral to the SOW or provided as an attachment. (Attachment A contains instructions and Attachment B a template for preparing the QASP). Following is suggested language for non-performance based services acquisitions where a detailed Quality Assurance Surveillance Plan is not required:* ***Quality Assurance Surveillance Plan. The COTR will review, for completeness, preliminary or draft products that the Contractor submits, and may return them to the Contractor for correction. Absence of comments by the COTR will not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of products required herein shall be by letter of approval and acceptance by the COTR. The Contractor shall not construe any letter of acknowledgment of receipt of products as a waiver of review, or as an acknowledgment that a product is in conformance with this work statement. Any approval given during preparation of a product, or approval for shipment shall not guarantee the final acceptance of the completed product.***

## 16. Post-Award Administration

*Discuss monitoring and milestones to be used for evaluation of Prime Contractors progress. Discuss any formal management systems to be used to monitor the Prime Contractor. Delineate the timing of periodic status reports. Include the requirements for Past Performance Evaluations to be completed at least annually and at the end of the task.*

## 17. Evaluation Criteria

*List the evaluation criteria for this SOW. At a minimum the criteria must be listed AND DESCRIBE the following criteria:*

1. Past Performance

2. Technical/Management Approach (including Quality Assurance if not broken out into a separate criterion)

3. Quality Assurance (including suitability of the QASP when requiring contractor to develop it as a part of their proposal for a performance-based effort)

4. Cost/Price

*A statement must be made regarding the relative importance of each evaluation criterion. This may be accomplished though the use of an adjective description or the assignment of weights, at the discretion of the customer.*

## Attachment A

# INSTRUCTIONS TO COMPLETE QUALITY ASSURANCE SURVEILLANCE PLAN (QASP) TEMPLATE

## 1. Introduction

a. The following documents are references:

   i. The Federal Acquisition Regulation (FAR), Subparts 37-6, Performance-Based Acquisition, and 46-4, Government Contract Quality Assurance.

   ii. HHS Acquisition SuperSite, Desk References and Performance Support, http://knownet2.com/agency_portals_hhs.htm.

b. Quality measurement and verification are required elements of all government contracts. The government is required to establish a QASP for service contracts and especially performance-based contracts. The QASP consists of four parts:
   - Deliverable to be completed (what will be monitored?)
   - Performance standard (what is expected?)
   - Acceptable quality level (AQL)/compliance level (what constitutes acceptance?)
   - Surveillance method/frequency (how will you perform your check: random sampling, customer complaint, etc.?)

c. The government is also required to evaluate and document performance progresses. Specific and objective performance standards will be established wherever possible. Task order performance surveillance will be performed in accordance with the terms of the contract (which the task order is written against) and the Task Order's QASP. The QASP describes how performance will be measured against the performance standards; it details the performance evaluation factors. These factors are usually stated in terms of:
   - Quality
   - Completeness
   - Timeliness
   - Cost Savings
   - Accuracy
   - Efficiency
   - Effectiveness

## 2. Purpose

a. The QASP is developed to comply with FAR Subparts 37-6, Performance-Based Acquisition, and 46-4, Government Contract Quality Assurance. In addition, FAR Subpart 46.103, Contracting Officer Responsibilities, states that agencies shall develop quality assurance surveillance plans when acquiring services. Note however, the development of a more formal QASP (including performance standards, acceptable quality levels, surveillance methods, and incentives and remedies) is only required for performance-based service contracts. The QASP for service contracts can be greatly simplified and streamlined based on the complexity of the services being acquired. These plans recognize the responsibility of the Service Provider (SP) to carry out its quality obligations, and contain measurable inspection and acceptance criteria corresponding to the performance standards contained in the statement of work. The QASP focuses on the level

of performance required by the statement of work, rather than the methodology used by the SP to achieve that level of performance.

b. The QASP is a government document used to specify the inspection and acceptance requirements of the Task Order SOW. For this reason, it is necessary that the Task Order's SOW and QASP be written in conjunction with each other (FAR Subpart 46.103 requires the CO to receive the QASP from the same activity responsible for technical requirements).

c. It is the government's responsibility to develop a QASP and conduct a quality assurance (QA) program with sufficient rigor to ensure mission accomplishment and efficiency.

d. For commercial services, the QASP shall be consistent with any existing commercial practices.

## 3. Direction

To the extent possible, the attached templates will be used. The contractor should consider the requirements therein when preparing the submission.

The Government may either prepare the QASP or require the offerors to submit a proposed QASP for the Government's consideration in development of the Government's plan (FAR Subpart 37.604).

Inspection will occur according to the schedule described in the Summary Planning Table (Table 1) and modified as required. When the SP's QC program proves to works well, and performance is consistently good, the amount of the surveillance can be decreased. If the SP has not equaled or exceeded the AQL, performance is considered unsatisfactory and the COTR/PO should prepare a SPDR and increase the oversight. Caution must be exercised to ensure that the surveillance results are accurate and applied to the correct performance period in which the work was produced.

Accurate and thorough surveillance and documentation is required for an effective and auditable QASP. Surveillance documentation and reports (usually monthly) prepared by the COTR/PO will be maintained in the COTR/PO file. The COTR/PO file will also contain a copy of the contract, all contract amendments, modifications, surveillance reports, SPDR Forms and other documentation required by the ACO.

Easy to use and complete documents are required; the management and surveillance team must be disciplined in filling out the required documents. The inspection and acceptance of SP products and services should be based upon clearly stated criteria and not opinion and anecdotal evidence. Completeness, currency, and accuracy are required to document both satisfactory and unsatisfactory performance. This QASP directs at least the following documents be used:

- The QASP Summary Planning Table (See Table 1)
  - Fill out one row of this table for each deliverable. (Fill out only one row for repeated deliverables, like periodic status reports.)
  - Provide a full description of the Performance Standard and the Acceptable Quality Level. This text may be of substantial length—write whatever is necessary to clearly state the Performance Standard and Acceptable Quality Level.

- The QASP Evaluation/Decision/Action Table (See Table 2)
  - Maintain this table, and all its supporting documents, as living documents, as separate, but companion documents to this QASP.
  - Fill out one row of this table for each SPECIFIC OCCURANCE of a deliverable.
  - Fill out a new row for each repeated deliverable, like periodic status reports.
  - Fill out a new row for each iteration of the same deliverable, and note this, for example, by designating it as "delivery #2."
  - Provide a full description in the remaining columns.

- Documentation of the SP performance:
  - Summary information (which includes a list of all deliverables, final and intermediate milestone and delivery dates, track to plan information, budget information, earned value (if required), risk management analysis by task and subtask, detailed budget information (to include budget to plan), evaluation criteria for each major definable deliverable, and/or other key indicators to measure the quality of the components delivered as part of the task order and
  - Periodic evaluations (minutes of the weekly or period determined by COTR/PO).

## 4. Implementation

The Evaluation/Decision/Action Table should be customized to meet the specific needs of the task order. Deliverables and the required delivery dates are specified in the Task Order. Milestones and additional subtasks may need to be established and monitored. The government needs to establish a surveillance program sufficient to monitor deliverable production schedule and quality. The government should also ensure that the SP has established internal methodology to both produce the deliverable and assure the government of progress.

The Contracting Officer's Technical Representative (COTR) is responsible for monitoring, assessing, recording, and reporting on the technical performance of the Contractor on a day-to-day basis and has primary responsibility for completing the QASP inspection, evaluation and documentation. It is extremely important for the COTR to establish and maintain a team-oriented line of communication with the Contractor's Project Manager (PM) and the PM's office staff when monitoring the SP functions. Meetings should be held on a regular basis in order to identify and resolve serious problems. Key outcomes of the meetings should be documented in the comments section of the QASP Evaluation/Decision/Action Table.

The contractor's performance should be evaluated by the COTR in terms of a specific set of products and activities, according to three categories: "superior," "acceptable," and "unacceptable." The criteria for each of the performance levels will be defined and discussed prior to the start of the task or subtask. In general, the work will be evaluated in terms of how well the requirements of the contract are satisfied, the extent to which the work performed follows the approach found in the contractor's technical proposal, clarity of documentation, and timeliness of scheduled task accomplishment.

The QASP records in Table 2 will substantiate the government's position in case the government seeks monetary deduction from the contractor for poor performance. If government action or lack of action caused the unsatisfactory performance, this also will be documented in the Evaluation/Decision/Action Table. A memorandum will be prepared by the COTR/PO explaining the government's action and submitted with the monthly report to the ACO.

Unsatisfactory contract performance will be reported immediately to the ACO and the contractor. The contractor is allowed to answer how the discrepancy will be corrected and how reoccurrence will be avoided. Appropriate supporting documentation will be forwarded to the ACO. A copy will be maintained in the COTR/PO file.

## Attachment B

## QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

**Task Order Title:**
**Task Order #:**
**As of: mm/dd/yyyy**

# 1. INTRODUCTION

*Note: Guidance is presented in italics with paragraph borders, while actual content is presented in normal font.* ***Please delete all guidance when finalizing the QASP.***

*Summarize Task Order (Task Order Title, Objectives, and Scope) here, replacing this comment with the summary.*

1.1 Purpose

This QASP specifically corresponds to the SOW Section 5, Specific Tasks. That Section discusses the requirements and standards of performance of the award. This document provides a surveillance plan sufficient to ensure SP performance and compliance with the FAR.

# 2. Surveillance Frequency and Sampling Method

2.1 Planning

The objective of this Surveillance Plan is to evaluate how the ___(Task Order Name)___ Task Order is being performed by ___(Service Provider)___ at __(Location)___.

*Provide a narrative in this section giving summary QASP information about each deliverable that will be evaluated. The entries should match the deliverables specified in the task order. Do not repeat the technical specification from the SOW for each subtask, but focus on narrating how you will carry out quality assurance on the deliverables. You may order these QASP deliverables in any sequence you find convenient, for example: in the narrative order of Section 5 of the SOW; in the order of the Deliverables Table of the SOW; in order by delivery date; in order by frequency of delivery. Replace this comment with the narrative.*

*Fill out the QASP Summary Planning Table (Table 1) based on the above narrative. Describe the quality assurance surveillance method that you will use for each deliverable. Also copy the same information into the Evaluation/Decision/Action Table (Table 2) as you need it—to be used when evaluating EACH SPECIFIC OCCURANCE of a deliverable. Table 1 is a planning table; Table 2 is an execution table. Quality Assurance methods include: Random Sampling, 100% Inspection, Scheduled Observations, Unscheduled Observations, User Survey, Validated User /Customer Complaints, Periodic Inspection, and Others as appropriate. (See references for definitions of the sample methods.)*
*Delete this comment.*

| QUALITY ASSURANCE SURVEILLANCE PLAN (QASP) | | | | | | |
|---|---|---|---|---|---|---|
| **Summary Planning Table** | | | | | | |
| **Task Order No.:** | | | | | | |
| **POC/Phone/E-Mail:** | | | | | | |
| **Del. No.** | **Deliverable Type** | **Performance Standard** | **Acceptable Quality Level** | **Method Used** | **Frequency** | **Incentive (+/-)** |
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |

**Table 1: Summary Planning Table**

The Summary Planning Table columns are filled in as follows:

Deliverable. No. — Number the Summary Table rows sequentially so they can be referred to in the Detailed Evaluation/Decision/Action Table.

Deliverable Type — Give a descriptive name of the deliverable, like Monthly Status Report; Management Plan; Software Design Specification; Transition Plan, etc.

Performance Standard — Using objective and measurable terms, describe the standard of quality you expect the deliverable to adhere to. For example, *restores desktop computer service within four hours of receiving trouble report during business hours*.

Acceptable Quality Level — State what level of quality for a deliverable will make it an acceptable deliverable. For example, *meets performance standard 95% of the time*.

Method Used — Explain how you will inspect deliverables to determine if the performance standard is met. Methods include 100% inspection (often used for written products), random or scheduled inspections, testing, etc.

Frequency — State how often inspections will take place.

Incentive (+/-) — If you choose to use incentives for a particular deliverable, state the criteria for applying them. For example, if a deliverable has an AQL of 95%, you may choose to pay an incentive fee if the performance standard is met 100% of the time in a particular period. Alternatively, you may choose to reduce payment if the performance standard is met less than 80% of the time in a particular period.

| QUALITY ASSURANCE SURVEILLANCE PLAN (QASP) | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Detailed Evaluation/Decision/Action Table** | | | | | | | | | | | | | | |
| **Task Order No.:** | | | | | | | | | | | | | | |
| **POC/Phone/E-Mail:** | | | | | | | | | | | | | | |
| **Ref. Del. No.** | **Each Deliverable Instance or Re-Delivery** | **Perf Std** | **Acceptable Quality Level** | **Method Used** | **Freq** | **Incentive (+/-)** | **Eval. Date** | **Compliance Level** | **Causative Factor** | **Effect on Mission** | **Action Required** | **Date Action Req. By** | **Rpt. No.** | **Comment** |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Table 2: Detailed Evaluation/Decision/Action Table**

**Table 2: Detailed Evaluation/Decision/Action Table**

The Detailed Evaluation/Decision/Action Table columns are filled in as follows:

| | |
|---|---|
| Reference Deliverable. No. | Use the number in the Summary Table for the deliverable type being evaluated. |
| Deliverable Type | Use the same descriptive name of the deliverable as used in the Summary Table. Add any information necessary to make it unique, like the date of a monthly status report, or re-delivery information about a second or subsequent delivery of the same product. |
| Performance Standard | Summarize the standard of quality stated in the Summary Table. |
| Acceptable Quality Level | Summarize the AQL stated in the Summary Table. |
| Method Used | Summarize the method description stated in the Summary Table. |
| Frequency | Repeat the frequency of inspection stated in the Summary Table. |
| Incentive (+/-) | Summarize the incentive description stated in the Summary Table. |
| Evaluation Date | Give the date of the specific evaluation. For recurring deliverables, give the date of the particular instance of the deliverable. For re-deliveries, give the date of the re-delivery. |
| Compliance Level | Results of the evaluation. Report this in the same objective and measurable terms used to state the performance standard. |
| Causative Factor | If the evaluation is not satisfactory, explain any causative factors. |
| Effect on Mission | If the evaluation is not satisfactory, explain any impact on the mission. |
| Action Required | If the evaluation is not satisfactory, explain any action needed. Resubmission of a deliverable may be one possibility. |
| Date Action Required By | This action date should be in alignment with any statements in the SOW as to redelivery requirements. |
| SPDR No. | If a Service Provider Discrepancy Report has been created, record its number here. |
| Comment | Add any explanatory comments that may be appropriate. |