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.

The customer may use the U.S. mail, fax, or e-mail to provide the TORP, except where indicated that a hard copy of a signed document is required. NITAAC expects delivery of documents in printed form and soft copy on INTEL PC 3.5" floppy. When customers use e-mail, NITAAC expects soft copy to be in MS Word or WordPerfect and MS EXCEL or Lotus 123.

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.

5.1.3 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

Describe the IT security required for the specific work to be done.

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

DHHS customers should be careful to address security requirements as documented in the DHHS Automated Information System Security Program (AISSP) Handbook. Consistent with the AISSP, the following subsections should be included in DHHS statements of work if applicable.

10.1 Information Technology Systems Security

DHHS customers must include this subsection if the task order involves, in whole or in part, Information Technology (IT) where the contractor will develop or have access to an Automated Information System (AIS), and is subject to the security requirements of the DHHS AISSP.

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

(a) **Sensitivity and Security Level Designations.**

The Statement of Work (SOW) requires the successful offeror to develop or access a Federal Automated Information System (AIS). Based upon the security guidelines contained in the *Department of Health and Human Services (DHHS) Automated Information Systems Security Program (AISSP) Handbook,* the Government has determined that the following apply:

(1) Category of Safeguarded Information

The safeguarded agency information that the successful offeror will develop or access is categorized as:

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

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

(2) Security Level Designations

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

The information that the successful offeror will develop or access is designated as follows:

Level ___ applies to the sensitivity of the data.
Level ___ applies to the operational criticality of the data.

The overall Security Level designation for this requirement is **Level ___**.

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

(3) Position Sensitivity Designations

Prior to award, the Government will determine the position sensitivity designation for each contractor employee that the successful offeror proposes to work under the task order. For proposal preparation purposes, the following designations apply:

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

[ ] Level 6C: Sensitive - High Risk (Requires Suitability Determination with a BI).
Contractor employees assigned to a Level 6C position are subject to a Background Investigation (BI).

[ ] Level 5C: Sensitive - Moderate Risk (Requires Suitability Determination with NACIC).
Contractor employees assigned to a Level 5C position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), or possibly a Limited Background Investigation (LBI).

[ ] Level 4C: Classified (Requires Special Access Clearance with an SSBI).
Contractor employees assigned to a Level 4C position are subject to a Single Scope Background Investigation (SSBI).

[ ] Level 3C: Classified (Requires Top Secret Clearance with an SSBI).
Contractor employees assigned to a Level 3C position are subject to a Single Scope Background Investigation (SSBI).

[ ] Level 2C: Classified (Requires Confidential or Secret Clearance with an LBI).
Contractor employees assigned to a Level 2C position shall undergo a Limited Background Investigation (LBI).

[ ] Level 1C: Non Sensitive (Requires Suitability Determination with an NACI).
Contractor employees assigned to a Level 1C position are subject to a National Agency Check and Inquiry Investigation (NACI).

Contractor employees who have met investigative requirements within the past five years may only require an updated or upgraded investigation.

*** (**NOTE:** The AISSP Handbook in Section XIV.D.4.d states that contractors are to pay the cost of required security background investigations. If this requirement is not applicable to your task order, please delete the sentence below. (This requirement is not explicitly included in NIH/NCI contracting forms, which are the source for Section 10 of the this Sample SOW.) ***

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

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

The offeror's proposal must:

(1) Include a detailed outline (commensurate with the size and complexity of the requirements of the SOW) of its present and proposed IT systems security program;

(2) Demonstrate that it complies with the AISSP security requirements, the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems;" and the DHHS AISSP Handbook.

At a minimum, the offeror's proposed information technology (IT) systems security program must address the minimum requirements of a **Security Level *___** identified in the DHHS AISSP Handbook, Exhibit III-A, Matrix of Minimum Security Safeguards.

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

(3) Include an acknowledgment of its understanding of the security requirements.

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

(c) **Required Training for IT Systems Security**

DHHS policy requires that contractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.

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

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

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

*** (**NOTE:** Include below when a prospective offeror will require access to sensitive information in order to prepare an offer, e.g. an offeror must access an NIH computer room floor plan. If this is not applicable to your solicitation, delete the entire subparagraph (d) below.) ***

(d) **Prospective Offeror Non-Disclosure Agreement**

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

*** (**NOTE:** Provide a description of the sensitive information and select the appropriate Position Sensitivity designation.) ***

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

[ ] Level 6C: Sensitive - High Risk
[ ] Level 5C: Sensitive - Moderate Risk

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

(1) Submit a written request to the Contracting Officer identified in the solicitation;
(2) Complete and submit the "Prospective Offeror Non-Disclosure Agreement" available on the NITAAC Website; and
(3) Receive written approval from the Contracting Officer.

Prospective offerors are required to process their requests for access, receive Government approval, and then access the sensitive information within the period of time provided in the solicitation for the preparation of offers.

Nothing in this provision shall be construed, in any manner, by a prospective offeror as an extension to the stated date, time, and location in the solicitation for the submission of offers.

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

(e) **References**

The following documents are electronically accessible:

(1) OMB Circular A-130, Appendix III: http://csrc.ncsl.nist.gov/secplcy/a130app3.txt
(2) DHHS AISSP Handbook: http://irm.cit.nih.gov/policy/aissp.html
(3) DHHS Personnel Security/Suitability Handbook: http://www.hhs.gov/ohr/manual/pssh.pdf
(4) NIH Applications/Systems Security Template: http://irm.cit.nih.gov/security/secplantemp.html
(5) NIST Special Publication 800-16, "Information Technology Security Training Requirements:" http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf
(6) NIH CIT-Policies, Guidelines and Regulations:
Table 1 - Categories of Safeguarded Agency Information: http://irm.cit.nih.gov/security/table1.htm
Table 2 - Security Level Designations for Agency Information: http://irm.cit.nih.gov/security/table2.htm
Table 3 - Positions Sensitivity Designations for Individuals Accessing Agency Information: http://irm.cit.nih.gov/security/table3.htm

10.2 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.

Disclosure of the information/data, in whole or in part, by the Contractor can only be made after the Contractor receives prior written approval from the Contracting Officer. Whenever the Contractor is uncertain with regard to the proper handling of information/data under the contract, the Contractor shall obtain a written determination from the Contracting Officer.

10.3 Information Technology Systems Security Specifications

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

Note: For more information about IT Security requirements see Chapters VII and XIV of the DHHS AISSP Handbook, including Exhibits VII-B, XIV-C and XIV-D. IF THIS IS NOT APPLICABLE TO THE TASK ORDER, DELETE THIS SUBSECTION.

The contractor agrees to comply with the IT systems security and/or privacy specifications set forth herein; the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the DHHS Automated Information Systems Security Program (AISSP) Handbook, which may be found at the following websites:

Computer Security Act of 1987: **http://csrc.ncsl.nist.gov/secplcy/csa_87.txt**
OMB A-130, Appendix III: **http://csrc.ncsl.nist.gov/secplcy/a130app3.txt**
DHHS AISSP Handbook: **http://irm.cit.nih.gov/policy/aissp.html**

The contractor further agrees to include this provision in any subcontract awarded pursuant to this task order. Failure to comply with these requirements shall constitute cause for termination.

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of the SOW. The contractor shall establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive Government information, data, and/or equipment.

In addition, during all activities and operations on Government premises, the contractor shall comply with DHHS, including Operational Division, rules of conduct.

a. Required IT Systems Security Training

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

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

*** (NOTE: The language contained within the brackets in the paragraph below is suggested only. The CO may choose to require this listing to be submitted separately or in another manner. The only requirement is that this listing must be submitted to the Project Officer as well as the Contracting Officer. If you choose to require this as a separate report, make sure that the task order provides specific instructions on the submission of the report,.e.g. under Section 9, Deliverables/Delivery Schedule, and possibly Section 5.1, Contract-Level and Task Order (TO) Management.) ***

The contractor shall maintain a listing by name and title of each individual working under this task order that has completed the required security training. Any additional security training completed by contractor staff shall be included on this listing. [The listing of completed training shall be included in the first technical progress report. (See SOW status reporting requirements.) Any revisions to this listing as a result of staffing changes shall be submitted with next required technical progress report.]

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

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

[List the required training courses here.]

b. Position Sensitivity Designations

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

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

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

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

Level 6C: Sensitive - High Risk (Requires Suitability Determination with a BI).
Contractor employees assigned to a Level 6C position are subject to a Background Investigation (BI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 5C: Sensitive - Moderate Risk (Requires Suitability Determination with NACIC).
Contractor employees assigned to a Level 5C position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), or possibly a Limited Background Investigation (LBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 4C: Classified (Requires Special Access Clearance with an SSBI).
Contractor employees assigned to a Level 4C position are subject to a Single Scope Background Investigation (SSBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 3C: Classified (Requires Top Secret Clearance with an SSBI).
Contractor employees assigned to a Level 3C position are subject to a Single Scope Background Investigation (SSBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 2C: Classified (Requires Confidential or Secret Clearance with an LBI).
Contractor employees assigned to a Level 2C position shall undergo a Limited Background Investigation (LBI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Level 1C: Non Sensitive (Requires Suitability Determination with an NACI). Contractor employees assigned to a Level 1C position are subject to a National Agency Check and Inquiry Investigation (NACI).

*** (List applicable Contractor Position Titles here if considered appropriate.) ***

Contractor employees in AIS-related positions shall comply with the DHHS criteria for the assigned position sensitivity designations prior to performing any work under this task order.

Contractor employees who have met investigative requirements within the past five years may only require an updated or upgraded investigation. Verifications of completed investigations (e.g. copies of certificates of investigations or security clearances), as well as requests for new investigations, shall be submitted to the Project Officer.

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

c. Commitment to Protect Sensitive Information

(1) Contractor Agreement

The Contractor shall not release, publish, or disclose sensitive information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of sensitive information:

-18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
-18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
-Public Law 96-511 (Paperwork Reduction Act)

(2) Contractor-Employee Non-Disclosure Agreements

Each contractor employee who may have access to sensitive information under this task order shall complete the "Contractor Employee Non-Disclosure Agreement" available on the NITAAC Website.

A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer prior to performing any work under the task order.

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.

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.*

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
3. 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.