DEPARTMENT OF HEALTH & HUMAN SERVICES Public Health Service

National Institutes of Health (NIH)
National Institute of Allergy and Infectious Diseases (NIAID)
Office of Cyber Infrastructure and Computational Biology (OCICB)
5601 Fishers Lane, MSC 9812
Rockville, MD 20852-9812

FROM: Thomas Reardon, NIAID Alternate ISSO, OCICB, NIAID

SUBJECT: Acquisition Plan for the project entitled,

_____

TO:

_____

ISSO Review and Certification of this requirement is required PRIOR to release of the resulting RFP. A copy of the complete AP package has been attached to this request.

The following information should be completed by the ISSO and returned to the Contracting Officer.

INFORMATION SYSTEMS SECURITY OFFICER (ISSO) PRESOLICITATION REVIEW AND RECOMENDATION

I have reviewed the statement of work for the subject project and have determined that the requirement ☐ contains, or, ☐ does not contain, a significant IT component with respect to connection to Federal AIS and/or access to sensitive data. My signature certifies that those requirements found to contain a significant IT component adequately specify the appropriate security requirements necessary to sufficiently protect the Government's interests in compliance with all Federal and DHHS security requirements as prescribed by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems," and the *DHHS Secure One,* or, should be modified as stated in this recommendation. The security requirements are set forth in such a manner that all prospective contractors can readily understand what is required, or, should be modified as stated in this recommendation.

The successful proposal(s) ☐ requires, or, ☐ does not require ISSO review for proposal compliance.

The successful proposal(s) ☐ requires, or, ☐ does not require an "Authorization to Operate" (ATO) certification by the NIAID Chief Information Officer.

_____ _____
ISSO, NIAID, NIH, DHHS Date

☐ **INFORMATION SECURITY IS NOT APPLICABLE** for this RFP.

RFP/CONTRACT PROVISIONS

It has been determined that the contractor personnel will develop of access federal automated information systems. Therefore, the NIAID ISSO recommends use of the following Section H provisions in the resulting RFP/Contract:

☐ **INFORMATION SECURITY**

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

a. Information Type

☐ **Administrative, Management and Support Information:**

☐ **Mission Based Information:**

b. Security Categories and Levels

******* (NOTE: The resultant contract will include the Security Categories and Levels, however for the purposes of this RFP, the Security Categories and Levels are specified in SECTION L.2.b. Technical Proposal Instructions of this RFP.) *******

Confidentiality	Level:	☐ Low	☐ Moderate	☐ High
Integrity	Level:	☐ Low	☐ Moderate	☐ High
Availability	Level:	☐ Low	☐ Moderate	☐ High
Overall	**Level:**	☐ **Low**	☐ **Moderate**	☐ **High**

c. Position Sensitivity Designations

(1) The following position sensitivity designations and associated clearance and investigation requirements apply under this contract:

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

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

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

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

Upon receipt of the Government's notification of applicable Suitability Investigation required, the contractor shall complete and submit the required forms within 30 days of the notification. Additional submission instructions can be found at the "NCI Information Technology Security Policies, Background Investigation Process" website: http://ais.nci.nih.gov.

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

(3) Contractor employees shall comply with the DHHS criteria for the assigned position sensitivity designations prior to performing any work under this contract. The following exceptions apply:

Levels 5 and 1: Contractor employees may begin work under the contract after the contractor has submitted the name, position and responsibility of the employee to the Project Officer, as described in paragraph c.(2) above.

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

d. Systems Security Plan

The contractor shall protect Federal automated information systems that are developed or accessed by the contractor. System security shall be accomplished in accordance with the contractor's System Security Plan dated _____. The plan must:

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

[OR** (To be determined during negotiations)**]

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

(i) Security Awareness Training
(ii) Logical Access Control

-Network (ex: firewall)
-System (ex: network OS, tcp wrappers, SSH)
-Application (ex: S-LDAP, SSL)
-Remote Access (ex: VPN)
-Monitoring and support (ex: IDS, pager, NOC)

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

(iv) Malicious Code Protection (ex: Antivirus, filtering of e-mail attachments, etc)

(v) Physical Security
-Access control (ex: locks, guards)
-Power conditioning and/or UPS
-Air conditioning
-Fire protection

Include an acknowledgment of its understanding of the security requirements.

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

e. Rules of Behavior

The contractor shall comply with the DHHS Rules of Behavior set forth in **DHHS Information Security Program Policy Handbook, Appendix G** at: http://intranet.hhs.gov/infosec/docs/policies_guides/ISPPH/PG_ISHbkv2_11_12_2004.pdf and the **NIH Information Technology General Rules of Behavior** at https://ocio.nih.gov/InfoSecurity/training/Pages/nihitrob.aspx.

f. Information Security Training

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

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

g. Personnel Security Responsibilities

The contractor shall perform and document the actions identified in the "Employee Separation Checklist", attached and made a part of this contract, when a contractor employee terminates work under this contract. All documentation shall be made available to the Project Officer and/or Contracting Officer upon request

h. Commitment to Protect Departmental Information Systems and Data

(1) Contractor Agreement

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

-18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
-18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)

-Public Law 96-511 (Paperwork Reduction Act)

(2) Contractor-Employee Non-Disclosure Agreements
Each contractor employee who may have access to sensitive Department information under this contract shall complete Commitment To Protect Non-Public Information - Contractor Agreement. A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer prior to performing any work under the contract.

i. References

DHHS Information Security Program Policy: http://www.hhs.gov/ohr/manual/pssh.pdf
DHHS Personnel Security/Suitability Handbook: http://www.hhs.gov/ohr/manual/pssh.pdf
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
NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems: http://csrc.nist.gov/publications/nistpubs/index.html
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
NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, Volume II: http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V2-final.pdf
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
NIH Computer Security Awareness Training Course: http://irtsectraining.nih.gov/
Roster of Employees Requiring Suitability Investigations: http://ais.nci.nih.gov/forms/Suitability-roster.xls
NCI Information Technology Security Policies, Background Investigation Process: http://ais.nci.nih.gov/
NIH Systems Security Plan Template (detailed): http://irm.cit.nih.gov/security/secplantemp.doc
NIH Systems Security Plan Outline (outline only): http://irm.cit.nih.gov/nihsecurity/Security_Plan_Outline.doc
NIH Information Technology General Rules of Behavior: http://irm.cit.nih.gov/security/nihitrob.html
Commitment To Protect Non-Public Information - Contractor Agreement: http://irm.cit.nih.gov/security/Nondisclosure.pdf

☐ ELECTRONIC AND INFORMATION TECHNOLOGY STANDARDS

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L.105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Final Standards can be accessed at http://www.access-board.gov/.

☐ ENERGY STAR REQUIREMENTS

Executive Order 13123, "Greening the Government Through Efficient Energy Management" and FAR 23.203 require that when Federal Agencies acquire energy using products, they select, where life-cycle cost-effective, and available, ENERGY STAR® or other energy efficient products.

Unless the Contracting Officer determines otherwise, all energy-using products acquired under this contract must be either an ENERGY STAR® or other energy efficient product designated by the Department of Energy's Federal Energy Management Program (FEMP).

For more information about ENERGY STAR® see http://www.energystar.gov/
For more information about FEMP see http://www.eere.energy.gov/

☐ **ACCESS TO NATIONAL INSTITUTES OF HEALTH (NIH) ELECTRONIC MAIL**

All Contractor staff that have access to and use of NIH electronic mail (e-mail) must identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, the contractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent.

☐ **OTHER**