INFORMATION SECURITY PROGRAM REQUIREMENTS

Checklist and Certification

RFP No: _____ **Pre Solicitation Review Date: _____**

Contract No:_____ **Pre-Award Review Date: _____**

Project Title: _____

Contracting Officer:_____
[Name and Contact Information]

PRE-SOLICITATION

[ ] INFORMATION SECURITY IS NOT APPLICABLE for this RFP.

[ ] INFORMATION SECURITY IS APPLICABLE and the following information is required for RFP preparation:

A. INFORMATION TYPE

[ ] Administrative, Management and Support Information:

[ ] Mission Based Information:

B. SECURITY CATEGORIES AND LEVELS

Confidentiality:	**[ ]** Low	**[ ]** Moderate	**[ ]** High
Integrity:	**[ ]** Low	**[ ]** Moderate	**[ ]** High
Availability:	**[ ]** Low	**[ ]** Moderate	**[ ]** High
Overall:	**[ ] Low**	**[ ] Moderate**	**[ ] High**

C. POSITION SENSITIVITY DESIGNATIONS

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

[ ] Tier 5: Critical Sensitive and Special Sensitive National Security, including Top Secret, SCI, and "Q" access eligibility.
[ ] Tier 5SR: Reinvestigation.

[ ] Tier 4: High Risk Public Trust (HRPT).
[ ] Tier 4SR: Reinvestigation.

[ ] Tier 3: Non-Critical Sensitive, National Security, including Secret and "L" access eligibility.
[ ] Tier 3SR: Reinvestigation.

[ ] Tier 2S with Subject Interview: Moderate Risk Public Trust (MRPT).
[ ] Tier 2SR: Reinvestigation.

[ ] Tier 1: Low Risk, Non-Sensitive, including HSPD-12 Credentialing.

D. PROSPECTIVE OFFEROR NON-DISCLOSURE AGREEMENT

[ ] Offerors **WILL NOT** require access to sensitive information in order to prepare an offer.
[ ] Offerors **WILL** require access to sensitive information in order to prepare an offer:

Description of sensitive information:

_____

_____

_____

_____

Select appropriate position sensitivity designation below.

[ ] Tier 4: High Risk Public Trust (HRPT).
[ ] Tier 2S with Subject Interview: Moderate Risk Public Trust (MRPT).

CERTIFICATION: Based on the above, and contingent upon inclusion of all applicable solicitation language prescribed in the NIH Workform, we certify that the solicitation specifies appropriate security requirements necessary to protect the Government's interest and is in compliance with all Federal and DHHS security requirements.

_____ _____
Project Officer Signature Date

_____
Project Officer Typed Name

_____ _____
Information Systems Security Officer Signature Date

_____
Information Systems Security Officer Typed Name

INFORMATION SECURITY PROGRAM REQUIREMENTS
Checklist and Certification

RFP No: _____ **Pre Solicitation Review Date: _____**

Contract No:_____ **Pre-Award Review Date: _____**

Project Title: _____

Contracting Officer:_____
[Name and Contact Information]

_____

PRE-AWARD

A. SYSTEMS SECURITY PLAN (SSP)

[ ] SSP Approved. The SSP dated _____, submitted by the Contractor has been reviewed by the Government, is considered acceptable, and should be incorporated into the awarded contract.

[ ] This project requires a full SSP conforming to the NIST Guide for developing Security Plans for federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf which must be submitted to the I/C, ISSO no later than 30 calendar days after the effective date of the contract.

[ ] The SSP submitted by the Contractor does not meet the minimum requirements for IT Security in the following area(s):

- **[ ]** Security Awareness Training
- **[ ]** Access Control
- **[ ]** Protection against data loss
- **[ ]** Malicious Code Protection
- **[ ]** Physical Security

A revised SSP shall be submitted no later than 90 calendar days after the assignment of task (eg. hosting a government website) that would require such a plan.

[ ] No SSP is required for this work.

B. OFFEROR'S PROPOSAL

[ ] Notwithstanding the information regarding the SSP, above, the offeror's proposal dated_____, specifies appropriate security requirements necessary to comply with the Federal and Departmental policy.

[ ] The offeror's proposal dated, _____ is deficient in the following areas:

_____

_____

_____

_____

[ ] No Award is recommended until the offeror submits additional information to resolve the deficiencies sited above.

[ ] Award may be made contingent upon the inclusion of contract language stipulating the submission of additional information resolving the deficiencies cited above. This information must be submitted no later than 30 calendar days after the effective date of this contract.

CERTIFICATION: Based on the above, and contingent upon inclusion of all applicable Contract language prescribed in the NIH Contract Workform, we certify that the contract specifies appropriate security requirements necessary to protect the Government's interest and is in compliance with all Federal and DHHS security requirements.

_____ _____

Project Officer Signature Date

_____

Project Officer Typed Name

_____ _____

Information Systems Security Officer Signature Date

_____

Information Systems Security Officer Typed Name