Appendix A. Information Security Certification Checklist

HHS Procurement Requirement - Internal Use Only

This Certification Checklist applies to and must be completed for all procurements involving acquisition of information, products, services, etc. This Checklist is for internal use only and will not be included in the package of documents submitted to Contractor. This Certification Checklist includes Part A, Part B, and Part C and involves a coordinated effort among the Requiring Activity Representative, Security, Privacy, and the Program Manager (and any other applicable personnel). The Requiring Activity Representative must submit the draft Certification Checklist to the Chief Information Security Officer (CISO) or designee, who will complete and sign Part A and to the Privacy Act Officer or designee who will complete and sign Part B. Both Security and Privacy personnel must complete Part C if applicable for their specific solicitation. The Requiring Activity Representative must ensure that all required parties complete a Certification Checklist in the early stages of the procurement life-cycle. If not all information is available at pre-awardstage of the contract, it must be included post-award. Submit completed Checklist or questions to the CISO Mailbox at **CISO@cms.hhs.gov**.

Acquisition Plan: ☐ HHS Acquisition Plan ☐ CMS Streamlined Acquisition Plan

Solicitation/Contract Number: _____

Pre-Solicitation Review Date: _____

Project Title: _____

Contracting Officer/Representative: _____

Cyber Risk Advisor: _____

Privacy Act Officer _____

System/Data Owner or Program Manager: _____

High-level Summary of the Solicitation:

Description of Design, Development, or Operation Work (if applicable):

Cloud Services will be: ◯ **Required** ◯ **Permitted** ◯ **Forbidden**

Information Security Categorization – Part A

Final Contract Requirements Review

◯ **Information security is not applicable. Provide a brief summary why information security does not apply and proceed to the signature page and include this form with the solicitation.**

◯ **Information security is applicable and the following information is required for use in the final contract:**

INFORMATION SECURITY CATEGORIZATION

(NOTE: Categorize the system and/or information by selecting the appropriate information type(s) below. Then, provide the overall risk rating in Table 2 by using the highest watermark of the security impact levels from the selected information types.

Security Categorization Level:

Check box next to appropriate information type(s)	Information Type	Confidentiality	Integrity	Availability	Digital Identity
☐	Investigation and intelligence-related, and security information	High	High	Moderate	**IAL 3/ AAL 3**
☐	Mission-critical information	High	High	High	**IAL 3/ AAL 3**
☐	Information about persons and Other Federal Information	Moderate	Moderate	Moderate	**IAL 2/ AAL 2**
☐	Financial, budgetary, commercial, proprietary and trade secret information	Moderate	Moderate	Moderate	**IAL 2/ AAL 2**
☐	Internal administration and Operational Information	Moderate	Moderate	Moderate	**IAL 2/ AAL 2**
☐	New technology or controlled scientific information	Moderate	Moderate	Low	**IAL 2/ AAL 2**

Check box next to appropriate information type(s)	Information Type	Confidentiality	Integrity	Availability	Digital Identity
☐	System configuration management information	Moderate	Moderate	Moderate	**IAL 2/ AAL 2**
☐	Other sensitive information	Low	Low	Low	**IAL 2/ AAL 2**
☐	Public information	Low	Low	Low	**IAL 2/AAL 2 or None**

Table 1: Information Types and Risk Ratings

Project/System Name	Confidentiality (Low, Moderate, High)	Integrity (Low, Moderate, High)	Availability (Low, Moderate, High)
Overall Risk: (Low, Moderate, High)			

Table 2: Information/System Categorization and Overall Risk

DIGITAL IDENTITY RISK ASSESSMENT

CMS has used the Digital Identity guidelines set forth by HHS and NIST and have aligned the IAL and AAL levels to the above data types. *FAL* would still need to be selected by the system, if they are utilizing a federated architecture

The Digital Identity IAL and AAL Levels for these information types is included in the table above. The *FAL* levels will be calculated at the system level.

• FAL – Federated Assurance Level corresponds to the strength of the assertion protocol used in federated environments to communicate authentication and attribute information to a relying party (RP) (Note: This only applies when federated architectures are utilized).

Based on the required level of assurance determined by the table, select the appropriate authentication level of assurance and authentication method required to access the information system, including remote authentication.

System Identity Assurance Level (IAL): ○ **IAL1** ○ **IAL2** ○ **IAL3**
System Authentication Assurance Level (AAL): ○ **AAL1** ○ **AAL2** ○ **AAL 3**
System Federated Assurance Level (FAL): ○ **FAL1** ○ **FAL2** ○ **FAL3**
--applies only to federated systems--

POSITION SENSITIVITY DESIGNATION/SENSITIVE INFORMATION

The ISSO, CISO, or representative, in coordination with the requiring activity representative and Personnel Security Offices, will determine the applicable position designations using OPM's Position Sensitivity Designation Automated Tool, which is located at https://www.opm.gov/investigations/, HHS Security Clearance Processes available at https://intranet.hhs.gov/about-hhs/national-security/security-clearance-processes, and Personal Security/Suitability Handbook available at https://intranet.hhs.gov/sites/default/files/s3fs-public/s3fs-public/2019-06/ONS%20PSSH.pdf. The following are position sensitivity levels that may apply to this solicitation/contract:

Investigation			Position Requirement
OLD		NEW	
NAC		NAC	NATIONAL AGENCY CHECK
Level 1 non-sensitive	NACI	Tier 1	Low Risk, Non-Sensitive, including HSPD-12 Credentialing
Level 5 moderate risk Public Trust	MBI	Tier 2S WITH SUBJECT INTERVIEW	Moderate Risk Public Trust (MRPT)
		TIER 2SR (REINVESTIGATION)	
Level 2 non-critical sensitive	NACLC & ANACI	Tier 3	Non-Critical Sensitive, National Security, including SECRET & "L" access eligibility
		TIER 3R (REINVESTIGATION)	
Level 6 high-risk Public Trust	BI	Tier 4 TIER 4R (REINVESTIGATION)	High Risk Public Trust (HRPT)
Level 3 critical-sensitive	SSBI	Tier 5 TIER 5 (REINVESTIGATION)	Critical Sensitive and Special Sensitive National Security, including Top Secret, SCI, and "Q" access eligibility
Level 4 special sensitive			Combined with T5

Tier _____

Sensitivity Level _____

Information Privacy Certification – Part B

Final Contract Requirements Review

Upon notification from the Requiring Activity Representative, the Privacy Act Officer or desginee shall complete this form. The purpose of this form is to determine the Privacy Act requirements and language to be included in this solicitation.

☐ Privacy Act applies to this contract (i.e., records are maintained in a system about individuals and retrieved from that system by name or other personal identifier). Provide a brief summary of Privacy Act records as required in the contract (e.g., personnel and payroll records about HHS employees; access control records about HHS employees, contractors, other system users and visitors; financial records about HHS obligors/obliges).

If Privacy Act requirements apply, complete the following information. This information is needed to tailor Section 3 upon inclusion in the SOW as required by the HHSAR "Privacy Act" clause, 352.224-70:

Applicable Statement of Records Notice (SORN) number(s), or statement indicating that a SORN will be developed:

Records disposition instructions:

Part C - Non-Disclosure Agreement (NDA)

PROSPECTIVE OFFEROR NON-DISCLOSURE AGREEMENT

◯ Offerors WILL NOT require access to sensitive information in order to prepare an offer and will not need a Non-Disclosure Agreement.

◯ Offerors WILL require access to sensitive information in order to prepare an offer. A Non-Disclosure Agreement (NDA) is necessary for a prospective offeror who will require access to government information in order to prepare the offer (i.e. a prospective offer must access an HHS computer room floor plan).

ATTESTATION: I hereby attest that the above information is true and accurate to the best of my knowledge.

Program Manager Signature: _____

Stop Here! Send the form to CISO@cms.hhs.gov for review and processing.
CO/COR signatures on page 8 should be completed after CISO/SOP signature.

Information Security and Privacy Certification
To be completed by the CISO Office

Based on the information provided and the analysis by the CRA and Privacy Advisor for this solicitation it has been determined that the following sections are required:

Selection	Section Name
☐	Section 2: Procurements Requiring Information Security and/or Physical Access Security
☐	Section 3: Requirements for Procurements Involving Privacy Act Records
☐	Section 4: Procurements Involving Government Information Processed on GOCO or COCO Systems
☐	Section 5: Contracts Involving Cloud Services
☐	Section 6A: Hardware Procurements
☐	Section 6B: Non-Commercial and Open Source Computer Software Procurements
☐	Section 6C: Information Technology Application Design, Development, or Support
☐	Section 6D: Physical Access to Government Controlled Facilities

CERTIFICATION: Based on the above, and contingent upon inclusion of all applicable language prescribed in the solicitation, I certify that the solicitation specifies appropriate security/privacy requirements necessary to protect the Federal Government's interests and is in compliance with all Federal, HHS and CMS security and privacy requirements.

Chief Information Security Officer (CISO) or Designee Signature :_____

Privacy Act Officer or Designee Signature: _____

Information Security and Privacy Acknowledgment

ACKNOWLEDGMENT: Based on the above, and contingent upon inclusion of all applicable security and privacy language prescribed, I acknowledge the above Information Security and Privacy Certification.

Contracting Officer (CO) Signature: _____

Contracting Officer Representative (COR) Signature: _____