Appendix A. Information Security Certification Checklist

HHS Procurement Requirement - Internal Use Only

This security and privacy checklist includes Part A and Part B. Part A should be completed in coordination with the ISSO, System Owner, and/or Program/Project Manager, and signed by the CMS Chief Information Security Officer (CISO) or designee. Part B should be completed by the requiring activity in coordination with the Privacy Advisor, Data Owner and/or Program/Project Manager, and signed by the CMS Senior Official for Privacy (SOP) or designee. The purpose of this form is to determine if the procurement 1) requires information security, 2) involves personally identifiable information (PII) or 3) is subject to the Privacy Act. This Checklist is for internal use only and will not be included in the package of documents submitted to the Contractor. This Checklist should be completed to accompany a Request for Proposal (RFP), Request for Quote (RFQ), or other procurement document. 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 Advisor: _____

System/Data Owner or Program Manager: _____

High-level Summary of the Solicitation:

Cloud Services will be Used: ○ **YES** ◉ **NO**

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 (Number and Title)	Confidentiality	Integrity	Availability	e-Authentication Level
☐	Investigation, intelligence-related, and security information (14 CFR PART 191.5(D))	High	High	Moderate	Level 4
☐	Mission-critical information	High	High	High	Level 4
☐	Information about persons	Moderate	Moderate	Moderate	Level 2 or Level 3
☐	Financial, budgetary, commercial, proprietary and trade secret information	Moderate	Moderate	Moderate	Level 3
☐	Internal administration	Moderate	Moderate	Moderate	Level 3
☐	Other federal agency information	Moderate	Moderate	Low	Level 3
☐	New technology or controlled scientific information	Moderate	Moderate	Low	Level 3

Check box next to appropriate information type(s)	Information Type (Number and Title)	Confidentiality	Integrity	Availability	e-Authentication Level
☐	Operational information	Moderate	Moderate	Moderate	Level 3
☐	System configuration management information	Moderate	Moderate	Moderate	Level 3
☐	Other sensitive information	Low	Low	Low	Level 2
☐	Public information	Low	Low	Low	None or Level 1

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

E-AUTHENTICATION RISK ASSESSMENT

Conduct an E-Authentication Threshold Analysis (E-Auth TA) to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary by following the OMB 04-04, E-Authentication Guidance for Federal Agencies (https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf) and NIST SP 800-63, Electronic Authentication Guideline. If a full E-auth RA is required, determine the level of assurance. The potential levels of assurance are:

- Level 1: Little or no confidence in the asserted identity's validity;
- Level 2: Some confidence in the asserted identity's validity;
- Level 3: High confidence in the asserted identity's validity; or
- Level 4: Very high confidence in the asserted identity's validity.

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

Level of Assurance: ◯ **N/A** ◯ **Level 1** ◯ **Level 2** ◯ **Level 3** ◯ **Level 4**

Authentication Method: ◯ **N/A** ◯ **Single-Factor** ◯ **Two-Factor** ◯ **Multi-Factor**

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. A Non-Disclosure Agreement (NDA) is necessary for a prospective offeror who will require access to government information in order to prepare an offer.

POSITION SENSITIVITY DESIGNATION/SENSITIVE INFORMATION

ISSO, CISO, or representative, in coordination with the requiring activity representative and Personnel Security Offices, determine the applicable position designations using the National Background Investigation Service (NBIS) Automated Tool for each Position Title, which is located at: https://pdt.nbis.mil/. The position sensitivity levels that apply to this solicitation/contract are:

Tier _____

Sensitivity Level _____

Information Privacy Certification – Part B

Final Contract Requirements Review

○ No PII[1] is involved in the final contract. Provide additional detailed information if applicable and proceed to the signature page.

◉ The final contract involves PII[2]. Please describe the PII that will be created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed as required in the solicitation. Complete the checklist and sign below.

☐ Privacy Act applies to the final contract. (e.g., it involves records about individuals retrieved by personal identifier). Provide a brief summary of Privacy Act records as required in the solicitation.

[1] PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016). Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother's maiden name, biometric records, etc.

[2] The E-Government Act of 2002 Section 208 (E-Government Act) and Office of Management and Budget (OMB) Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of 2002, form the core of the Privacy Impact Assessment (PIA) requirement. Together, they state that a PIA is an assessment of how information is handled within certain electronic systems. Each PIA should consider: 1) Whether the system complies with legal, regulatory, and policy requirements related to privacy; 2) The risks and effects of how that system handles personally identifiable information (PII); and 3) How the system could be changed to mitigate potential privacy risks. The Department of Health and Human Service (HHS) has chosen to evaluate the privacy implications of all electronic systems regardless of whether the E-Government Act or OMB M-03-22 requires a PIA.

PRIVACY ACT

If Privacy Act requirements apply, complete the following information. This information, plus the design, development or operation work description (Page 1) is needed to tailor 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:

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

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:

Section	Applicability	Examples of Requirements
Section 2 ☐	All procurements requiring information security and/or physical access	Will develop or have the ability to access user or host government information. Safeguarding sensitive information mandatory training; incident response encryption etc....
Section 3 ☐	Procurements Involving records that are or will be subject to the Privacy Act of 1974 (5 U.S. Code 552a)	An acquisition is subject to the Privacy Act if it involves a system of records, meaning records about individuals retrieved by name or other personal identifier.
Section 4 ☐	Procurements involving: GOCO (systems owned by the Government and operated by a contractor ; COCO (systems owned and operated by the contractor	Information processed on GOCO or COCO facilities. Information Security Requirements include: FISMA Compliance; obtaining an Authority to Operate prior to deployment or implementation; An initial/annual security control assessment; and continuous monitoring.
Section 5 ☐	Procurements Involving: • Infrastructure as a Service • Platform as a Service • Software as a Service • Information Systems moving to a Cloud Environment	Cloud Services Provider solicitations purchased either Directly or when bundled with another vendors offering.
Section 6	Procurements Involving: • Hardware Acquisitions (Server Computer peripherals etc...) • Non-Commercial/Open Source Computer Software • IT Application Design and Support	Information Technology Design, Development, and support. Server Computer peripherals etc..., Application Helpdesk support; secure coding etc...
6A ☐		
6B ☐		
6C ☐		

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 :_____

Senior Official for Privacy (SOP) 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: _____