

Centers for Medicare & Medicaid Services  
 Information Security and Privacy Group

CMS Security and Privacy Language for Information and Information Technology Procurements

Final

Version 2.0

July 1, 2022

# Summary of Changes

The table below capture changes when updating the document. All columns are mandatory.

| Version Number | Date | Chapter Section | Author/Owner Name | Description of Change |
| --- | --- | --- | --- | --- |
| *1* | *10/18/2019* | *All* | *ISPG* | *Initial Publication* |
| *1.1* | *6/9/2020* | *4 and 5* | *ISPG* | *Updated POA&M and Vulnerability mitigation timelines, along with updated TLC information* |
| *2.0* | *7/1/2022* | *All* | *ISPG* | *Updated to reflect HHS new policy release* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Table of Contents

[Summary of Changes ii](#_Toc106363051)

[Table of Contents iii](#_Toc106363052)

[1. Purpose 1](#_Toc106363053)

[2. Background 1](#_Toc106363054)

[3. Scope 1](#_Toc106363055)

[4. Authorities 3](#_Toc106363056)

[2. Procurements Requiring Information Security and/or Physical Access Security 4](#_Toc106363057)

[3. Requirements for Procurements Involving Privacy Act Records 13](#_Toc106363058)

[4. Procurements Involving Government Information Processed on GOCO or COCO Systems 15](#_Toc106363059)

[5. Contracts Involving Cloud Services 22](#_Toc106363060)

[6. Other IT Procurements 28](#_Toc106363061)

[Appendix A. Information Security Certification Checklist 31](#_Toc106363062)

[Appendix B. Prospective Offeror Non-Disclosure Agreement 32](#_Toc106363063)

[Appendix C. Contractor Non-Disclosure Agreement 34](#_Toc106363064)

[Appendix D. List of Deliverables 35](#_Toc106363065)

[Appendix E. References 38](#_Toc106363066)

[Appendix F. Acronyms 43](#_Toc106363067)

[Appendix G. Definitions of Key Terms 45](#_Toc106363068)

# Purpose

The HHS Policy for Information Technology Procurements - Security and Privacy Language aligns with the Federal Acquisition Regulation (FAR) [1], the HHSAR, [2] and other federal and HHS policies. The purpose of this Policy is to mandate the standard security and privacy language for information and information technology (IT) procurements throughout HHS. This document also includes procedures guidance to assist Contracting Officers (COs), CO Representatives (CORs), Program Managers (PMs), and other stakeholders in selecting the appropriate security and privacy language to include in acquisition documents (e.g., Performance Work Statement (PWS), Statement of Work (SOW), etc.) pre-award and post-award of the contract. The goal is to better prepare contractors and service providers to be compliant with HHS and federal security and privacy requirements, avoiding unnecessary future contract modifications. This Policy includes the information security and privacy requirements, referred to as standard contract language in this document, to ensure federally mandated security and privacy controls and standards are met throughout the Department of Health and Human Services (HHS). Operating Divisions (OpDivs) may customize this Policy to include OpDiv specific information, create their own policy, or supplement the standard contract language herein, provided the OpDiv standard contract language is compliant with and is as restrictive as the baseline contract language.

# Background

To protect its information resources, HHS is responsible for implementing and administering an information security program in compliance with applicable public laws, federal regulations, and Executive Orders. This includes the Federal Information Security Modernization Act (FISMA) of 2014 and Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource. To meet these requirements, the Department has issued the HHS Information Security and Privacy Policy (IS2P), which contains the policies to secure information and information systems throughout the Department.

While the IS2P is the overarching policy governing IT security and privacy at HHS, it does not provide explicit guidance for the Contracting Officer (CO), Contracting Officer Representative (COR), Requiring Activity Representative, and other staff involved in the procurement of information and IT products and services. Therefore, the HHS Policy for Information Technology Procurements - Security and Privacy Language has been developed to guide federal employees and/or contractors (and/or subcontractors) who need to address requirements for procurements that involve information and IT products and services and standardize the security and privacy contract language across the Department. This includes services, which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions.

Effective November 30, 2005, the Civilian Agency Acquisition Council and the Defense Acquisition Regulation Council agreed to amend the FAR to incorporate the FISMA security requirements for all federal agencies. Thus, agency heads must ensure all agency personnel involved with IT procurements understand how to meet FISMA and OMB Circular A-130 requirements, as well as standards and guidance set forth by the National Institute of Standards and Technology (NIST) guidelines [3]. In addition, the Federal Information Technology Acquisition Reform Act (FITARA) [4], enacted in 2014, mandate that government agencies' Chief Information Officers (CIOs) have a significant role in IT procurements decisions and oversight.

# Scope

This *Policy* contains baseline requirements and standard security and privacy language to be used in procurement documentation (e.g., SOW, PWS, etc.) when acquiring information and information technology. This *Policy* supplements federal and HHS acquisition regulations (See Appendix E - References). Only the Office of the Assistant Secretary for Financial Resources (ASFR)/Office of Acquisitions (OA), in conjunction with Office of the Chief Information Officer (OCIO), may issue HHS acquisition policy.

In addition, designated healthcare components (hereinafter referred to as covered components) within HHS that are subject to the regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA)[[5]](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn5) and the Health Information Technology for Economic and Clinical Health (HITECH) Act,[[6]](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn6) must ensure that their contracts with entities that qualify as their business associates include all required business associate provisions per 45 Code of Federal Regulations (CFR) 164.504(e) and breach reporting policies and procedures for suspected or confirmed breaches of protected health information. Such contracts must impose a duty to cooperate with the covered component and/or the Department's breach investigation and response, and must require all subcontractors to be contractually bound to the same privacy, security and breach-related terms and conditions as a condition of receiving [government/federal] data. Four divisions within HHS have been designated as healthcare components under HIPAA by the HHS Secretary: 1) CMS, insofar as it operates the fee-for-service Medicare program; 2) the Program Support Center (PSC's) Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers; 3) the World Trade Center (WTC) Health Program and 4) the Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions. More information about requirements for business associates and sample contract language may be found on the Office for Civil Rights (OCR) Website.[[7]](https://intranet.hhs.gov/policy/hhs-policy-information-technology-procurements-security-and-privacy-language#ftn7)

The Requiring Activity Representative and contracting office, in coordination with the OpDiv Information System Security Officer (ISSO), Senior Official for Privacy (SOP), System Owner and the Chief Information Security Officer (CISO), must ensure procurement documentation includes the applicable security and privacy language with sufficient details to enable Contractors and service providers to fully understand the requirement. The Requiring Activity Representative must also ensure sufficient information regarding security and privacy regulations, mandates, and requirements to which they will be subject under the contract or task order that may be awarded to them are understood. The directions in the beginning of each section explicitly detail the applicable language to specific acquisition types. The acquisition types include:

* Procurements requiring information security and/or physical access;
* Procurements involving personally identifiable information (PII) or records of individuals;
* Procurements involving government-owned/contractor-operated (GOCO), contractor-owned/ contractor-operated (COCO);
* Procurements involving cloud services;
* Other procurement types
  + Hardware,
  + Non-commercial and open source software,
  + Information technology application design, development or support.

The terms procurement and acquisition are similar and are used interchangeably throughout this document.

This *Policy* does not supersede any other applicable law or higher-level agency directive or policy guidance.

# Authorities

The following are the primary authoritative sources driving the requirements in this *Policy*:

* Buy American Act, 41 U.S.C. §§ 8301-8305, July 15, 2019.
* Federal Acquisition Regulation (FAR), as amended.
* Federal Acquisition Supply Chain Security Act (FASCSA) of 2018.
* Federal Information Security Modernization Act of 2014 (FISMA), December 2014.
* Federal Information Technology Acquisition Reform Act (FITARA), as amended.
* Office of Management and Budget (OMB), Circular A-130, Managing Information as a Strategic Resource, July 2016.
* Public Law 115-232 § 889, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, August 13, 2018.
* Public Law 115-390, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act.
* United States Code (U.S.C.) of Federal Regulation (CFR), as amended.

# Procurements Requiring Information Security and/or Physical Access Security

**DIRECTIONS**

The language set forth in the subsections of **Section 2** applies to ALL solicitations and contracts for procurements requiring information security and/or physical access security. A procurement requires security if, as a result of the procurement, any contractor (and/or any subcontractor) employee:

* will develop; have the ability to access, use, or host; and/or maintain government information[[1]](#footnote-2) and/or government information system(s), including instances of remote access to or physical removal of such information beyond agency premises or control; or
* will have regular or prolonged physical access to a “federally-controlled facility,” as defined in FAR Subpart 2.1.[[2]](#footnote-3)

Physical and Logical Access refers to when contractor personnel (and/or any subcontractor) are expected to have (1) routine physical access to a *CMS*-controlled facility; (2) logical access to a *CMS* -controlled information system; (3) access to government information, whether in a *CMS* -controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3) as per the HHSAR Subpart 304.13 – Personal Identity Verification[[3]](#footnote-4) and OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.*[[4]](#footnote-5)

As part of the acquisition planning process, the appropriate Program Officials shall determine whether, based on the nature of the requirement, contractor personnel may require access to *CMS* -controlled facilities and/or information systems, including sensitive data/information, in order to perform the Contract/Statement of Work (SOW)/ Performance Work Statement (PWS). If contractor access is required, the requiring activity representative must assess, based on information available at that point in the process, the type, frequency, and duration of such access. Following that determination, the requiring activity representative shall consult with *CMS* and/or local building officials/staff, and officials/staff involved with personnel security, including the designated personnel security representative, to determine applicable security requirements and, as necessary, adjust project requirements to minimize security and access issues. The requiring activity representative shall comply with HSPD-12, FAR Subpart 4.13,[[5]](#footnote-6) and the applicable standard language below in making these judgments and determinations.

***The following definitions and clauses are relevant to this section:***

1. FAR clause 52.239-1, Privacy or Security Safeguards (Section 2.A.2.b.)

2. HHSAR Clause 352.224-71\*\* (Section 2.A.2.e.)

3. FAR 7.105(b)(5) (Section 2.A.7.)

4. FAR 11.002(g) (Section 2.A.7.)

5. FAR 52.239-1(c) (Section 2.D.3.b.)

6. FAR Subpart 4.13 (Section 2.F)

7. FAR Subpart 52.204-9 (Section 2.F)

*\*\* This clause should be tailored to either 1) list types of information that require confidentiality protection or 2) say “None” if the contract involves no information types that require confidentiality protection. If there are information types requiring confidentiality protections, the reasons for those restrictions must also be included.*

**Exceptions. Section 2** language below does not apply to procurements for only hardware and software licenses. These requirements are addressed in **Section 6** of this document.

The requiring activity representative must confer with its *CMS*’ CISO or designee to complete the checklist in [Appendix A](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Security-and-Privacy-Language-for-Procurements) (Part A and Part B) to determine *CMS* -specific requirements, and identify any additional security language applicable to the solicitation/contract.

Review **Sections 3, 4, and 5** to determine which additional language is applicable to your solicitation/contract.

**NOTE:** **The numbering scheme used in this document applies to THIS DOCUMENT ONLY, and those preparing solicitation and award documents should adjust the numbering accordingly.**

***Instructions appearing in italics in a text box are for the requiring activity and any other personnel preparing procurements documentation and should be removed by the document preparer.***

**Note: The language below shall be included in the Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or other purchase description. This language does not alleviate the requirement to properly incorporate applicable FAR and HHSAR clauses into the applicable contract clauses section of the solicitation and resultant contract.**

**START COPYING LANGUAGE BELOW**

1. Baseline Security Requirements
   1. **Applicability.** The requirements herein apply whether the entire contract or modification (hereafter "contract"), or portion thereof, includes either or both of the following:
      1. **Access (Physical or Logical) to Government Information:** A Contractor (and/or any subcontractor) will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.
      2. **Operate a Federal System Containing Information:** A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.
   2. **Safeguarding Information and Information Systems*.*** All government information and information systems must be protected in accordance with HHS*/* CMS policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:
      1. Protect the:
         * **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
         * **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
         * **Availability**, which means ensuring timely and reliable access to and use of information.
      2. Categorize all information owned and/or collected/managed on behalf of HHS/*CMS* and information systems that store, process, and/or transmit HHS information in accordance with FIPS 199 and National Institute of Standards and Technology ([NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf)Based on information provided by the ISSO, CISO, CMS SOP, or other representative, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:
         * **Confidentiality:**  [  ] Low [  ] Moderate [  ] High
         * **Integrity:**  [  ] Low [  ] Moderate [  ] High
         * **Availability:**  [  ] Low [  ] Moderate [  ] High
         * **Overall Impact Level:** [  ] Low [  ] Moderate [  ] High
      3. Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of HHS*/*CMSregardless of location or purpose.
      4. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s).
      5. Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS*/*CMS Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain all applicable security and privacy policies by contacting the CO/COR or HHS*/*CMS security and/or privacy officials.
   3. **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.
   4. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable HHS/CMS privacy policies, and complete all the requirements below:  
        
      1. Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "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." 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. Based on information provided by the ISSO, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:  
           
         [  ] No PII [  ] PII
      3. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed.  
         111
         * If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within *[CMS to insert contract-specific timeline]* after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.
         * The Contractor must support the agency in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.
   5. **Controlled Unclassified Information (CUI). Executive Order 13556 defines** CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,*part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling"*refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323.  The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:
      1. Marked appropriately;
      2. Disclosed to authorized personnel on a Need-To-Know basis;
      3. Protected in accordance with NIST SP 800-53,*Security and Privacy Controls for Information Systems and Organizations*applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171,*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and
      4. Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88*, Guidelines for Media Sanitization*.
   6. **Protection of Sensitive Information**. For security purposes, information is *or*may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
   7. **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.  
        
      The confidentiality, integrity, and availability of such information must be protected in accordance with HHS and CMS policies. Unauthorized disclosure of information will be subject to the HHS/CMSsanction policies and/or governed by the following laws and regulations:
      1. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
      2. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
      3. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
   8. **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
   9. **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.
   10. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.
   11. **Contract Documentation***.* The Contractor must use provided templates, policies, forms and other agency documents found at <https://security.cms.gov> to comply with contract deliverables as appropriate.  
         
       **Standard for Encryption.** The Contractor (and/or any subcontractor) must:
       1. Comply with the *HHS Standard for Encryption of Computing Devices and Information*to prevent unauthorized access to government information.
       2. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
       3. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and CMS-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
       4. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR *[CMS-provided delivery date]*.
       5. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys <http://csrc.nist.gov/publications/>. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.
   12. **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the CMS non-disclosure agreement. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.
2. Training Requirements
   1. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract must complete the applicable HHS/CMS Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete CMSInformation Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training must be compliant with HHS training policies.
   2. **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.
   3. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records must be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.
3. Rules of Behavior
   1. The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, and *HHS Rules of Behavior for Privileged Users*.
   2. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual CMS Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.
4. Incident Response
   1. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/CMSIRT teams **within 24 hours,** whether the response is positive or negative.  
        
      FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."
   2. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
      1. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
      2. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor must send CMS approved notifications to affected individuals in accordance with the CMS Breach Analysis Team (BAT) instruction.
      3. Report all suspected and confirmed information security and privacy incidents and breaches to the CMS Incident Response Team (IRT) *via the CMS Help Desk (410) 786-2580 or CMS IT Service Desk (cms\_it\_service\_desk@cms.hhs.gov)*, COR, CO, CMS SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable CMS and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:
         * Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
         * Not include any sensitive information in the subject or body of any reporting e-mail; and
         * Encrypt sensitive information in attachments to email, media, etc.
      4. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* and HHS/CMS privacy breach response policies when handling PII breaches.
      5. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation.
5. Position Sensitivity Designations  
   All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract:
6. Homeland Security Presidential Directive (HSPD)-12  
   The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*
7. Roster  
   The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within a timeframe to be determined by CMS of the effective date of this contract. Any revisions to the roster as a result of staffing changes must be submitted within a timeframe to be determined by CMS of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.  
     
   If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.
8. Contract Initiation and Expiration
   1. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology or the CMS SDLC, as amended and in accordance with the HHS Contract Closeout Guide (2012).
   2. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC and CMS SDLC that require artifact review and approval.
   3. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation in accordance with the CMS SDLC, as Amended to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.
   4. **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO withinas soon as possible or as determined by CMS before an employee stops working under this contract.
   5. **Contractor Responsibilities upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) must return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or CMS policies.
   6. The Contractor (and/or any subcontractor) must perform and document the actions identified the COR when an employee terminates work under this contract within30 calendar days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.
9. Records Management and Retention
   1. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *HHS Policy for Records Management* andCMS policies and must not dispose of any records unless authorized by HHS*/*CMS.
   2. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS*/*CMS policies.

High Value Asset (HVA)  
If a system is identified as HVA, the contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay in addition to the above requirements

**STOP COPYING LANGUAGE HERE**

# Requirements for Procurements Involving Privacy Act Records

**DIRECTIONS**

In addition to the standard baseline language in **Section 2**, the requiring activity representatives shall include the clauses and language set forth below in all solicitations and contracts involving records that are or will be subject to the Privacy Act of 1974 (5 U.S.C. 552a). Records are subject to the Privacy Act if they constitute a “system of records,” which is defined in the Privacy Act as records about individuals maintained in a system from which they are retrieved by name or other personal identifier.

Please be cognizant that not all information systems that contain personally identifiable information (PII) qualify as Privacy Act systems of records. The HHS/*CMS* Senior Official for Privacy (SOP) who completes [Appendix A](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Security-and-Privacy-Language-for-Procurements) must consult with the System/Data Owner and the *CMS* Privacy Act Contact, or the Departmental Privacy Act Officer within OS/ASPA, to determine if the procurement will involve records subject to the Privacy Act and, if so, to identify any existing government-wide, Department-wide, or *CMS* -specific Systems of Records Notices (SORNs) that cover the records, or to confirm if a new or revised SORN is needed. Existing SORNs are located by conducting an Internet search using “HHS SORNs” as the search term.

Be aware that subsection (i) of the Privacy Act prescribes criminal penalties for certain violations of the Privacy Act, including, for example, willfully operating a new system of records or making a significant change to an existing system of records before publishing a new or revised SORN describing the system or system change as required by subsection (e)(4) of the Act. Subsection (m) of the Privacy Act provides that the criminal liability provisions of subsection (i) apply to contractors, and to any employee of such contractors, when an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function. Subsection (m) requires that such contracts contain provisions that “cause” the requirements of the Privacy Act to apply to the affected systems of records.

***The following definitions and clauses are relevant to this section:***

1. FAR Subpart 24.101- Definitions. Consult the definitions of “agency,” “individual,” “maintain,” “operation of a system of records,” “record,” and “system of records on individuals” to determine if the Privacy Act applies. **If the Privacy Act applies, the following three clauses must be incorporated.**

2. FAR Clause 52.224-1 Privacy Act Notification.

3. FAR Clause 52.224-2 Privacy Act.

4. HHSAR Clause 352.224-70 Privacy Act. **NOTE:** This clause requires inclusion of Language specifying the applicable system(s) of records or proposed system(s) of records, the design, development, or operation work the Contractor is to perform, and the records disposition instructions to be followed by the Contractor upon completion of contract performance.

**If the Privacy Act applies, the Contracting Officer (CO)/CO Representative shall ensure that the language below is included in the Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or other purchase description. This language does not alleviate the requirement to properly incorporate the three FAR and HHSAR clauses identified in the box above into the applicable contract clauses section of the solicitation and resultant contract.**

**START COPYING LANGUAGE HERE**

1. Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals from which records are retrieved by name or other identifying particular.

The System of Records Notice that is applicable to this contract is: *[CMS insert SORN name/number if one exists. If there is no SORN, indicate that a new or revised SORN will be developed]*.

The system of records design, development, or operation work the Contractor is to perform is: *[CMS insert description of design, development, and/or operation work; see definitions in the FAR at 24.101 - Definitions]*.

The disposition to be made of the Privacy Act records upon completion of contract performance is: *[CMS insert records disposition instructions the contractor and any subcontractor must follow upon completion of contract performance]*.

**STOP COPYING LANGUAGE HERE**

# Procurements **Involving Government Information Processed on GOCO or COCO System**s

**DIRECTIONS**

The Federal Information Security Modernization Act (FISMA of 2014, (44 U.S.C. 101),[[6]](#footnote-7) Office of Management and Budget (OMB Circular A-130, *Managing Information as a Strategic Resource,[[7]](#footnote-8)* and Federal Procurements Regulation (FAR) 39.101[[8]](#footnote-9) mandate that contractor systems, including Government-Owned/Contractor-Operated (GOCO) or Contractor-Owned/Contractor-Operated (COCO) be at least as secure as Government systems operated by the Government.

Therefore, in addition to the standard language in **Section 2 and Section 3** (if applicable) above, the requiring activity representative will include the security language stated below in this **Section 4** in all solicitations/contracts involving GOCO/COCO as required by FAR Part 12 – Acquisition of Commercial Items, FAR Part 39 – Acquisition of Information Technology, including Subparts 39.1 and 39.2 and FAR Part 52 – Solicitation Provisions and Contract Clauses, including Subparts 52.239-1 and 52.204-21.

***In addition to definitions and clauses specified in Section 2 and applicable definitions and clauses in Section 3, the following definitions and clauses are relevant to this section:***

1. FAR Part 52 including clauses 52.239-1 and 52.204-21 (Section 4.A.)

2. FAR Subpart 39.101(c) (Section 4.5)(b.)

**NOTE**: **The selection of standard language below may be dependent on the contract level of effort. The requiring activity representative must collaborate with the Contracting Officer, System Owner, Senior Official for Privacy, ISSO, and/or** *CMS* **CISO, when preparing solicitations/contracts involving government information processed on GOCO or COCO systems to determine all applicable security and privacy language and if any additional security and privacy requirements apply to the solicitation/contract. For example, the Contractor may already have an existing ATO that can be leveraged or require a new ATO. In addition, the security control assessment may be conducted by the Government, Contractor, or independent third party depending on the level of risk and type of assessment required.** *CMS* **should strive to have contractors obtain independent third-party verification, but can accept contractor or government certifications, based on *CMS’* risk assessment. Agencies should establish controls consistent with the type of data being stored, collected, transmitted, or processed, and ensure the solicitation clearly articulates the requirements.**

**NOTE: The language below shall be included in the Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or other purchase description. This language does not alleviate the requirement to properly incorporate the applicable FAR and HHSAR clauses into the applicable contract clauses section of the solicitation and resultant contract.**

**START COPYING LANGUAGE BELOW**

1. Security Requirements for GOCO and COCO Resources
   1. **Federal Policies.** The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS policies that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P)*, *CMS Information Systems Security and Privacy Policy (IS2P2),* *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and*Organizations; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.
   2. **Assessment and Authorization (A&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) to be determined by CMS. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ CMS IS2P2*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach*(latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).  
        
      CMS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.
      1. **A&A Package Deliverables** - The Contractor (and/or any subcontractor) must provide an A&A package within as determined by CMS to the CO and/or COR. The following A&A deliverables are required to complete the A&A package :
         * **System Security Plan (SSP)** – due prior to the submission of the A&A package in order to request an ATO, based on the CFACTS format template. The SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and CMS policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least ***annually*** thereafter and if requested, provide a copy of the updated SSP.
         * **Security Assessment Plan/Report (SAP/SAR)** - due prior to the ATO.The security assessment must be conducted by a third-party assessor for High and Moderate systems, or by an independent assessor for Low systems and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and CMS policies. The assessor will document the assessment results in the SAR.  
             
           Thereafter, the Contractor, in coordination with CMS must assist in the assessment of the security controls initially and update the SAR at least ***annually***. A copy of the updated SAR should be provided if requested.
         * **Independent Assessment** – due as required by CMS.  The Contractor (and/or subcontractor) must have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all *"high"* deficiencies before submitting the package to the Government for accreditation and/or acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).
         * **POA&M** – due within 30 days after the independent third-party assessment final report approval and must be created in CFACTS. All critical-risk weaknesses must be mitigated within ***15 days,*** high-risk weaknesses must be mitigated within ***30 days***, medium weaknesses must be mitigated within ***90 days,*** and low weaknesses must be mitigated **365 days**, from the date the weaknesses are formally identified and documented. CMS will determine the risk rating of vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones and CMS policies. Depending on the severity of the risks, CMS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly** in CFACTS.
         * **Contingency Plan and Contingency Plan Test** – dueprior to the ATO and updated annually thereafter. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and CMS policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor must update and test the Contingency Plan at least ***annually***.
         * **E-Authentication Questionnaire** - The contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.  
             
           Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS/CMS policies.
      2. **Information Security Continuous Monitoring.** Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, must meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, HHS IS2P and CMS IS2P2.
      3. **Annual Assessment/Penetration (Pen) Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party.) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due dateto be determined by CMS.
      4. **Asset Management** - Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing HHS/CMS-owned information/data. It is anticipated that this inventory information will be required to be produced at leastevery 72 hours.IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.
      5. **Configuration Management** - Use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS*/*CMS upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
      6. **Vulnerability Management** - Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least every 72 hours.
      7. **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and CMS specified timeframes:
         * Critical vulnerabilities require patching to be released and remediated within 15 days
         * High vulnerabilities require patching to be released and remediated within 30 days
      8. **Secure Coding** - Follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
      9. **Boundary Protection** - The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
   3. **Government Access for Security Assessment**. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) must afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS/CMS, including but are not limited to:
      1. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.  
           
         The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.
      2. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.
         * Segregate Government protected information and metadata on the handling of Government protected information from other non-government information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.
         * Cooperate with inspections, audits, investigations, and reviews.
   4. **End of Life Compliance.** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the CMS CISO if it impacts only the CMS). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.
   5. **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) must ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS/CMS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:
      1. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with CMS, HHS encryption standard and current FIPS 140 validation certificate from the NIST CMVP.
      2. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), in accordance with Acceptable Risk Safeguards (ARS) control CM-6, Configuration Settings, other CMS settings requirements, and HHS Minimum Security Configuration Standards;
      3. Maintain the latest operating system patch release and anti-virus software definitions*;*
      4. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
      5. Automate configuration settings and configuration management in accordance with HHS/CMS security policies, including but not limited to:
         * Configuring its systems to allow for periodic HHS/CMS vulnerability and security configuration assessment scanning; and
         * Using Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
   6. **Rights to Data.** All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.
   7. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements**. The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:
      1. Develop rules for suppliers' development methods, techniques, or practices;
      2. Use of secondary market components;
      3. Prohibit counterfeit products;
      4. Dispose and/or retain elements such as components, data, or intellectual property securely;
      5. Ensure adequate supply of components;
      6. Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
      7. Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
      8. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
      9. Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
      10. Prohibit the use of covered telecommunications and video surveillance equipment or services.

**STOP COPYING LANGUAGE HERE**

# Contracts Involving Cloud Services

**DIRECTIONS**

In addition to the standard baseline language in **Section 2** and applicable language from **Sections 3 (Privacy)** and **4 (GOCO/COCO)**, the Contracting Officer or representative shall include the language set forth in the subsections of this **Section 5** in ALL solicitations and contracts for procurements involving cloud services. These include: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and information systems moving to a cloud environment. The requiring activity representative must confer with the CMS System Owner, ISSO or CISO, and CMS SOP to determine any additional security and privacy requirements applicable to the solicitation/contract that need to be included.

Cloud services solicitations/contracts, either directly with a Cloud Service Provider (CSP) or when cloud services are bundled with another vendor’s offerings, must:

1. Include Federal Risk and Authorization Management Program (FedRAMP) Standard Contract Clauses, FedRAMP Control-Specific Contract Clauses, and applicable HHS/CMS contract clauses to ensure that FedRAMP, HHS, and *CMS* security compliance, monitoring, and reporting requirements are addressed.
2. Establish a service level agreement (SLA) that defines:

* Performance metrics, how they will be monitored, and penalties for failure to meet them;
* Data management and disposition; and
* Roles, responsibilities, and reporting requirements.

For additional information, refer to the HHS Cloud Computing and Federal Risk and Authorization Management Program Guidance (<http://intranet.hhs.gov/it/cybersecurity/policies/index.html>)

***In addition to clauses specified in section 2 and applicable clauses in sections 3 and 4, the following clauses are apply to this section:***

1. FAR Part 24.104 (Section 5.A.)

2. FAR clause 52.239-1 (Section 5.F.2.)

**NOTE: Be aware that CSP may have standard SLAs that include incident response requirements and timelines that may be inconsistent with HHS’ requirements.** *CMS* **must ensure that the SLA will include the one-hour requirement for reporting incidents involving sensitive information in accordance with HHS’ incident response policy. This negotiation should also ensure the** *CMS* **is afforded access to the required systems, and other steps necessary to properly respond to an incident.**

The language below is based on the FedRAMP Standard Contract language, selected language from the FedRAMP Control-Specific Clauses referenced above, which has been modified for HHS contracts for cloud services, and HHS-specific security requirements. Consult the FedRAMP website for any updates to the standard issued documents and templates ([www.fedramp.gov](http://www.fedramp.gov)).

**NOTE: The language below shall be included in the Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or other purchase description. This language does not alleviate the requirement to properly incorporate the applicable FAR and HHSAR clauses into the applicable contract clauses section of the solicitation and resultant contract.**

**START COPYING LANGUAGE BELOW**

1. HHS FedRAMP Privacy and Security Requirements  
     
   The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:
   1. **FedRAMP Compliant ATO**. Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by a timeline determined by CMS.
      1. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline ([www.FedRAMP.gov](http://www.fedramp.gov/)). The *HHS Information Security and Privacy Policy (IS2P),* *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance*, and the CMS Information System Security and Privacy Policy (IS2P2) further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.
      2. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
   2. **Data Jurisdiction.** The contractor must store all information within the security authorization boundary, data at rest or data backup, within the Continental United States (CONUS) if so required.  Refer to G.x Contractor Work Performed Outside of the United States and its Territories (April 2016) in the Solicitation/Contract.
   3. **Service Level Agreements.** *Add when applicable* The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with CMS to develop and maintain an SLA.
   4. **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/CMS policies.
2. Protection of Information in a Cloud Environment
   1. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/CMS policies <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.
   2. HHS/CMS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS/CMS retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS/CMS and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS/CMS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to HHS/CMS.
   3. The Contractor (and/or any subcontractor) must ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS/CMS policies.
   4. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:
      1. Maintenance of links between records and metadata, and
      2. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.
   5. The disposition of all HHS/CMS data must be at the written direction of HHS/CMS. This may include documents returned to HHS/CMS control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.
      1. If the system involves the design, development, or operation of a system of records on individuals, the Contractor must comply with the Privacy Act requirements*.*
3. Assessment and Authorization (A&A) Process
   1. The Contractor (and/or any subcontractor) must comply with HHS/CMS and FedRAMP requirements as mandated by federal laws, regulations, and HHS/CMS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS*/*CMS security policies. The contractor must obtain authorization prior to deployment or service implementation.
      1. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation within CFACTS in a timeline to be determined by CMS. The agency ATO must be approved by the CMS authorizing official (AO) prior to implementation of system and/or service being acquired.
      2. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
      3. For all acquired cloud services, the A&A package must contain the following documentation:
         * Security Assessment Plan (SAP)/Security Assessment Report (SAR)
         * System Security Plan (SSP)
         * Plan of Action and Milestones
         * Contingency Plan and Contingency Plan Test
         * E-Authentication Questionnaire].

Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS*/CMS* policies using CMS templates and defined timelines*.*

* 1. HHS/CMS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS/CMS exercises this right, the Contractor (and/or any subcontractor) must allow HHS/CMS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS/CMS requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
  2. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the contractor must document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS/CMS may require remediation at the contractor's expense, before HHS/CMS issues an ATO.
  3. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the HHS POA&M Standard, from discovery: (1) critical vulnerabilities no later than ***fifteen (15) days*** and (2) high within **thirty (30) days** (3) medium within **ninety (90) days** and (4) low vulnerabilities no later ***than three hundred and sixty (360).***In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the timelines assigned to the POA&M within CFACTS. HHS/CMS will determine the risk rating of vulnerabilities using FedRAMP baselines.
  4. **Revocation of a Cloud Service**. HHS/CMS have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS/CMS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or CMS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

1. Reporting and Continuous Monitoring
   1. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities. Meetings shall be held at least monthly, or as needed.
   2. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis via the CCIC requirements which can be provided by contacting [EVM-CMP@cms.hhs.gov](mailto:EVM-CMP@cms.hhs.gov). Deliverables are identified as:
      1. Operating system, database, Web application, and network vulnerability scan results;
      2. Updated POA&Ms;
      3. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the CMS System Owner or AO; and
      4. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/CMS security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.
2. Configuration Baseline
   1. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS*/CMS* configuration baseline.
   2. The contractor must use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS/CMS and NIST defined configurations and do not alter these settings.
3. Incident Reporting  
   1. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS*/CMS]*, OMB, and US-CERT requirements and obtain approval from CMS. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.
   2. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS/CMS access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:
      1. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/CMS personnel, or agents acting on behalf of HHS/CMS*,*using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.
      2. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes at a minimum the following:
         * Company and point of contact name;
         * Contract information;
         * Impact classifications/threat vector;
         * Type of information compromised;
         * A summary of lessons learned; and
         * Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.
4. Media Transport
   1. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards)*.*
   2. All information, devices and media must be encrypted with HHS/CMS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.
5. Boundary Protection: Trusted Internet Connections (TIC)
   1. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.
   2. The contractor must route all external connections through a TIC.
   3. **Non-Repudiation**. The contractor must provide a system that implements encryption with current FIPS 140 validation certificate from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

**STOP COPYING LANGUAGE HERE**

# Other IT Procurements

**DIRECTIONS**

The following acquisition types are categories that are not covered by the sections stated above. These include hardware procurements, non-commercial/open source software procurements, and procurements involving information technology (IT) design, development and support.

*CMS* shall adhere to OMB M-16-20 *Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services* when acquiring mobile devices.

***The following clauses apply to this section:***

1. FAR Part 12 (Section 6.A.1.)

2. FAR Subpart 4.13 (Section 6.A.1.)

**NOTE: The Contracting Officer should confer with the System Owner, Information System Security Office (ISSO) and/or** *CMS* **Office of the Chief Information Security Officer (OCISO) when developing a contract involving other types of IT procurements to make sure all applicable security and privacy language is included.**

**NOTE: The language below shall be included in the Statement of Work (SOW), Statement of Objectives (SOO), Performance Work Statement (PWS), or other purchase description. FAR and HHSAR clauses are referred to in the solicitation and contract language herein. This language does not alleviate the requirement to properly incorporate such clauses into the applicable contract clauses section of the solicitation and resultant contract.**

**START COPYING LANGUAGE HERE**

1. Hardware Procurements  
   1. **Card Readers**. The Contractor (and/or any subcontractor) must include [Federal Information Processing Standard (FIPS) 201-compliant](https://www.idmanagement.gov/approved-products-list)) smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.
   2. **Mobile Devices**. The contractor must follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*and comply with Public Law 115-232 § 889*,* when purchasing mobile devices that process or store HHS/CMS data.

**STOP COPYING LANGUAGE HERE**

***(NOTE: The following are instructions for the Contracting Officer (CO) and other stakeholders when preparing acquisition documentation; not language to be included in contracts.)***

The use of non-commercial and open source computer software is in accordance with the HHS/*CMS* Guidance for Purchasing Noncommercial Computer Software and “Open Source” Licenses (2012),[[9]](#footnote-10) and OMB M-04-16, Software Acquisition.[[10]](#footnote-11)

If HHS/*CMS* wants to be able to use or distribute the computer software, it is imperative that the computer software, including the source code if it is required by the procuring program, be included as a deliverable.

Noncommercial computer software means software that does not qualify as commercial in nature (e.g., commercial items and commercial off the shelf (COTS) items as defined in FAR 2.101). The following language should be used as appropriate in noncommercial computer software contracts. Each section includes an instruction providing where the information should be included in the contract.

**START COPYING LANGUAGE BELOW**

1. Non-Commercial and Open Source Computer Software Procurements

The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by the United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP) that will limit system software vulnerability exploits. The contractor will be liable for malicious or defective code or failure to reduce risk.

***(NOTE: If this procurement involves handling of sensitive information, include language from Section 2 above.****)*

**STOP COPYING LANGUAGE HERE**

This section refers to procurements including application design, development, or support. For the purposes of this document, “computer software” means:

1. Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and
2. Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

“Computer software” does not include computer databases or computer software documentation.

**START COPYING LANGUAGE BELOW**

1. Information Technology Application Design, Development, or Support  
     
   1. The Contractor (and/or any subcontractor) must ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
   2. The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards, the Open Web Application Security Project (OWASP), and the *HHS Policy for Software Development Secure Coding Practices* that will limit system software vulnerability exploits.
   3. The Contractor (and/or any subcontractor) must ensure that computer software developed on behalf of HHS/CMS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor must test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS/CMS environment. No sensitive data must be used during software testing.
   4. The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS/CMS must be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

**STOP COPYING LANGUAGE HERE**

**(NOTE:** For procurements involving physical access to government facilities, selected language from Appendix B: Standards may apply. This includes, but not limited to security awareness, incident response, and HSPD-12. Consult with the OpDiv Information Systems Security Officer (ISSO), OpDiv Senior Official for Privacy (SOP) and other relevant stakeholders to select applicable language.)

Additionally, due to the COVID-19 Epidemic of 2020 (Effective as of March 30, 2020), The below contract language must be included in all COVID-19 contract actions until such time the HHS Secretary makes a determination to issue rated contracts related to items used for allowing HHS employees/contractors to physically use and/or operate in HHS facilities and spaces.

1. Physical Access to Government Controlled Facilities

"HHS reserves the right to exercise priorities and allocations authority with respect to this contract, to include rating this order in accordance with 45 CFR Part 101, Subpart A—Health Resources Priorities and Allocations System."

1. Information Security Certification Checklist

Please see fillable PDF available on the ISP Library.

1. Prospective Offeror Non-Disclosure Agreement

**(NOTE: To be completed by prospective offeror if access to sensitive information, non-public information, confidential information, and/or Controlled Unclassified Information (CUI) is required in order to prepare an offer.)**

*The CMS may modify this NDA to accommodate additional agency/contract requirements.*

Information and Information Technology Systems Security Non-Disclosure Agreement (NDA)

Solicitation No:

(Fill in the solicitation Number)

Project Title:

(Fill in Title from solicitation)

(*Organization’s name)*, intends to respond to the Government’s Solicitation/Project title indicated above. The Government has determined that the solicitation requires prospective offerors to have access to sensitive information in order to prepare an offer.

I, *(Offeror Official name and title),* of (*Organization’s name)*, on this day of , 20 , on behalf of my organization hereby request access to the sensitive information described in Section L.III. of the RFP cited above.

I, the undersigned, understand that the Government has determined that any individual having access to the sensitive information described in the solicitation must possess a valid and current Suitability Determination at the Level identified in Section L.III. of the RFP cited above.

I, the undersigned, do hereby affirm the following:

* I have a valid and current Suitability Determination sufficient to access the sensitive information (copy of suitability determination attached).
* I will be the corporate official solely responsible for appropriately safeguarding the sensitive information while in the possession of (Organization’s name);
* The sensitive information will be used solely for the purpose of preparing an offer;
* I will not release, publish, or disclose the sensitive information to unauthorized personnel; and
* I will protect the sensitive information and personally identifiable information in accordance with relevant federal laws, regulations and guidelines *[CMS, insert applicable laws if any.]*.

Signature of Prospective Offeror:

Name of Prospective Offeror:

Date:

Signature of Witness:

Name of Witness:

Date:

Copies Retained by: Contractor Official and Contracting Officer

1. Contractor Non-Disclosure Agreement



1. List of Deliverables

The following table details a listing of possible deliverables that may be completed by the Contractor (at a minimum) and included in the Schedule of Deliverables *[CMS specify process/format for submitting deliverables]*. **Please note that deliverables from Section 2 apply to Sections 3, 4, and 5.**

| Document Section | Deliverable Title/Description | Due Date | Applicable  (y/n) |
| --- | --- | --- | --- |
| 2 – Roster | Roster | *To be determined by CMS after contract award* |  |
| 2 – Contractor Employee Non-Disclosure Agreement (NDA) | Contractor Employee Non-Disclosure Agreement (NDA) | Prior to performing any work on behalf of HHS/*CMS* |  |
| 2 – Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA) | Assist in the completion of a PTA/PIA form | *To be determined by CMS after contract award* |  |
| 2 – Training Records | Copy of training records for all mandatory training | In conjunction with contract award and annually thereafter or upon request |  |
| 2 – Rules of Behavior | Signed ROB for all employees | Initiation of contract and at least annually thereafter |  |
| 2 – Incident Response | Incident Report (as incidents or breaches occur) | As soon as possible and without reasonable delay and no later than 1 hour of discovery |  |
| 2 – Incident Response | Incident and Breach Response Plan | Upon request from *CMS* |  |
| 2 – Personnel Security Responsibilities | List of Personnel with defined roles and responsibilities | *To be determined by CMS after contract award* |  |
| 2 – Personnel Security Responsibilities | Off-boarding documentation, equipment and badge when leaving contract | *To be determined by CMS after contract award* |  |
| 2 – Background Investigation | Onboarding documentation when beginning contract. | Prior to performing any work on behalf of *CMS* |  |
| 2 - Certification of Sanitization of Government and Government Activity-Related Files, Information, and Devices. | Form or deliverables required by *CMS*. | At contract expiration. |  |
| 2 – Contract Initiation and Expiration | If the procurement involves a system or cloud service, additional documentation will be required, such as Disposition/Decommission Plan | At contract expiration. |  |
| 4 – Security Assessment and Authorization (SA&A) | SA&A Package   * SSP * SAR * POA&M * Authorization Letter * CP and CPT Report * E-Auth (if applicable) * PTA/PIA (if applicable) * Interconnection/Data Use Agreements (if applicable) * Authorization Letter * Configuration Management Plan (if applicable) * Configuration Baseline * Other *CMS* -specific documents | *To be determined by CMS after contract award* |  |
| 5 – Protection of Information in a Cloud Environment | Contract expiration | *To be determined by CMS after contract award* |  |
| 5 – SA&A Process for Cloud Services | SA&A Package   * SSP * SAR * POA&M * CMP * CP and CPT Report * E-Auth (if applicable) * PTA/PIA (if applicable) * Penetration Test Results * Interconnection/Data Use/Agreements (if applicable) * Service Level Agreement * Authorization Letter * Configuration Management Plan (if applicable) * Configuration Baseline * Other *CMS* -specific documents | *To be determined by CMS after contract award* |  |
| 5 – Reporting and Continuous Monitoring | POA&M updates;  Revised security documentation/Agreements | *Quarterly/as requested by CMS* |  |
| 5 – Security Alerts, Advisories, and Directives | List of personnel with designated roles and responsibilities | *To be determined by CMS after contract award* |  |
| 5 – Incident Reporting | * Incident reports (as needed) * Incident Response Plan | *As needed in coordination with CMS Incident Management Team* |  |
| 6 – Other IT Procurements (Non-Commercial and Open Source Computer Software Procurements) | * Computer software, including the source code. | Prior to performing any work on behalf of *CMS* |  |

1. References
2. **Federal Laws, Directives and Policies**

United States Code (U.S.C.) of Federal Regulation (CFR), as amended (<http://www.ecfr.gov/cgi-bin/ECFR?page=browse>).

Federal Acquisition Regulation (FAR), as amended (<https://www.acquisition.gov/?q=browsefar>).

Federal Information Security Management Act (FISMA) of 2002 (Pub. L. No. 107-347, Title III) (<http://csrc.nist.gov/>).

Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. 101), as amended (<https://www.congress.gov/>).

Federal Information Technology Acquisition Reform Act (FITARA) H.R. 1232, as amended (<https://www.congress.gov/>).

Executive Order 13556 – *Controlled Unclassified Information (CUI)*, *(implemented at 3 CFR, Part 2002*), as amended (<https://obamawhitehouse.archives.gov/>).

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, as amended (<https://www.dhs.gov/>).

FedRAMP Standard Contract Clauses, as amended (http://www.fedramp.gov/).

FedRAMP Control-Specific Contract Clauses, as amended (http://www.fedramp.gov/).

The Health Insurance Portability and Accountability Act (HIPAA), as amended (https://www.hhs.gov/hipaa/for-professionals/index.html).

The Health Information Technology for Economic and Clinical Health Act (HITECH), as amended (<https://www.healthit.gov/>).

National Archives and Records Administration (NARA) Bulletin 20013-02 (2013), as amended (www.archives.gov).

National Industrial Security Program Operating Manual (NISPOM), as amended (https://intranet.hhs.gov/security/index.html).

Office of Personnel Management (OPM) Position Sensitivity Designation Automated Tool, as amended (<https://www.opm.gov/investigations/>).

The Privacy Act of 1974, as amended (<https://www.justice.gov/opcl/privacy-act-1974>).

Public Law 96-511 Paperwork Reduction Act of 1980, as amended (<https://www.gpo.gov/>).

United States Government Configuration Baseline (USGCB), as amended (<http://usgcb.nist.gov/>).

OMB Policy and Memoranda (https://obamawhitehouse.archives.gov/omb//)

OMB Circular A-130, *Managing Information as a Strategic Resource,* as amended.

OMB Encryption Guidance, as amended.

OMB M-17-12, *Preparing for and Responding to a Breach of PII.*

OMB Memorandum 07-18, *Ensuring New Procurements Include Common Security Configurations,* as amended.

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,*

OMB M-06-19, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

OMB M-06-15, *Safeguarding Personally Identifiable Information*.

OMB M-04-16, *Software Acquisition*.

OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.

OMB M-03-22,Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

1. **HHS Policy**

HHS Cloud Computing and Federal Risk and Authorization Management Program [FedRAMP] Guidance, as amended (<http://intranet.hhs.gov/it/cybersecurity/policies/>).

HHS Contract Closeout Guide, as amended, (<http://intranet.hhs.gov/abouthhs/contracts-grants-support/>).

HHS Enterprise Performance Life Cycle [EPLC], as amended (<http://www.hhs.gov/ocio/>).

HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications, as amended (<http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/>).

HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum, as amended (<http://intranet.hhs.gov/it/cybersecurity/policies/index.html>).

HHS-OCIO *Policy for Information Systems Security and Privacy Policy*, as amended (<http://intranet.hhs.gov/it/ocio/>).

HHS *Guidance for Purchasing Noncommercial Computer Software and “Open Source” Licenses,* as amended (<http://www.hhs.gov/ocio/policy/>).

HHS Standard for the *Definition of Sensitive Information*, as amended (<http://intranet.hhs.gov/it/cybersecurity/docs/policies_guides/>).

HHS Standard for Encryption of Computing Devices and Information, as amended (https://intranet.hhs.gov/it/cybersecurity/policies/index.html).

HHS *Standard for Plan of Action and Milestones*, as amended (<http://intranet.hhs.gov/it/cybersecurity/policies/>).

Health and Human Services Acquisition Regulation (HHSAR), as amended ([https://www.gpo.gov/fdsys/pkg/CFR-2015-title48-vol4/pdf/CFR-2015-title48-vol4-chap3.pdf](http://www.hhs.gov/grants/contracts/)).

HHS Personnel Security & Suitability Handbook, as amended (<http://intranet.hhs.gov/security/ossi/documents/>).

HHS Privacy Incident Response Team [PIRT] Standard Operating Procedures [SOP], as amended (<http://intranet.hhs.gov/it/cybersecurity/docs/>).

Rules of Behavior for use of HHS Information Resources, as amended (<http://www.hhs.gov/ocio/policy/>).

HHS Security and Privacy Language for Information and Information Technology Procurements v2, as amended (<https://intranet.hhs.gov/it/strategy-policy-governance/policies-standards-guides/standards/index.html>)

1. **NIST Guidance (**[**http://csrc.nist.gov/publications**](http://csrc.nist.gov/publications)**/)**

NIST IR 7511 Revision 4, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements,* as amended.

NIST SP 800-171 Rev 1, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,* as amended.

NIST SP 800-145, *The NIST Definition of Cloud Computing*, as amended.

NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* as amended.

NIST SP 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* as amended.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information,* as amended.

NIST SP 800-88 Rev 1, *Guidelines for Media Sanitization,* as amended.

NIST SP 800-64 Revision 2, *Security Considerations in the Information System Development Lifecycle,* as amended.

NIST SP 800-63-3, Digital Identity Guidelines: Authentication and Lifecycle Management.

NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide,* as amended.

NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) – Volume 1: Guide, Volume 2: Appendices*, as amended.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* as amended.

NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans,* as amended.

NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* as amended.

NIST SP 800-34 Revision 1, *Contingency Planning Guide for Information Technology Systems,* as amended.

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments,* as amended.

NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information System*s, as amended.

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems,* as amended.

FIPS PUB 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* as amended.

FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems,* as amended.

FIPS 140-2, *Security Requirements for Cryptographic Modules,* as amended.

1. **CMS Guidance**

CMS Information Systems Security and Privacy Policy (IS2P2), as amended (<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS-Information-Systems-Security-and-Privacy-Policy-IS2P2.html?DLPage=2&DLEntries=10&DLSort=0&DLSortDir=ascending>)

CMS Acceptable Risk Safeguards (ARS), as amended (<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-31-Publication.html?DLPage=1&DLEntries=10&DLSort=0&DLSortDir=ascending>)

CMS Target Life Cycle (TLC), as amended (<https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/TLC/index>)

1. Acronyms

|  |  |
| --- | --- |
| ASA | Assistant Secretary for Administration |
| ASFR | Office of the Assistant Secretary for Financial Resources |
| BI | Background Investigation |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| COR | Contracting Officers Representative |
| CSIRC | Computer Security Incident Response Center |
| CSIRT | Computer Security Incident Response Team |
| CSP | Cloud Service Provider |
| DA | Division of Acquisition |
| E-Auth | Electronic Authentication |
| FAR | Federal Acquisition Regulations |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Modernization Act of 2014 |
| FY | Fiscal Year |
| GB | GigaByte |
| HHS | Department of Health and Human Services |
| HHSAR | Health and Human Services Acquisition Regulations |
| HIPAA | Health Insurance Portability and Accountability Act |
| HSPD | Homeland Security Presidential Directive |
| IS2P | Information Systems Security and Privacy Policy |
| ISSO | Information Systems Security Officer |
| IT | Information Technology |
| M | Memorandum |
| MBI | Minimum Background Investigation |
| NARA | National Archives and Records Administration |
| NDA | Non-Disclosure Agreement |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OGAPA | Office of Grants and Acquisition Policy and Accountability |
| OMB | Office of Management and Budget |
| OpDiv | Operating Division |
| OSSI | Office of Security and Strategic Information |
| PII | Personally Identifiable Information |
| PIV | Personal Identification Verification |
| PL | Public Law |
| PM | Program Manager |
| RBT | Role Based Training |
| RFP | Request for Proposal |
| RoB | Rules of Behavior |
| SCAP | Security Content Automation Protocol |
| SORN | System of Record Notice |
| SOW | Statement of Work |
| SOP | Senior Official for Privacy |
| SP | Special Publication |
| SSP | System Security Plan |
| STAFFDIV | Staff Division |
| TBD | To be determined |
| USGCB | United States Government Configuration Baseline |
| USC | United States Code |

1. Definitions of Key Terms

**Definitions.** The following are definitions for key terms used throughout the document.

1. Authorizing Official (AO): Senior federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation (OMB Circular A-130).
2. Authorization to Operate (ATO): The official management decision given by a senior federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems (OMB Circular A-130).
3. Business Associate: A “business associate” is a person or entity, identified by the definition of the same term at 45 CFR 160.103, including those who other than a member of the workforce of a covered entity, perform functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A “business associate” also is a Contractor or subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)).
4. Confidential Information: Refers to information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization or the government (Sensitive Data/Information and HHSAR subpart 352.224-71 Confidential Information).
5. Controlled Unclassified Information (CUI): Controlled Unclassified Information' (CUI) means Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. (OMB Circular A-130).
6. Covered Contractor Information System: An information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information (FAR 52.204-21).
7. Deliverable: Quantifiable goods or services that will be provided upon the completion of a contract (HHS Defined).
8. Federal Contract Information: Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments. (FAR 52.204-21)
9. Government Information: Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form (OMB Circular A-130). Examples include grantee information, PII, PHI, financial information, etc. Often times also referred to as federal information.
10. Federal Information System: An information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency. (OMB Circular A-130).
11. Foreign National: An alien, i.e., any person who is not a citizen of the United States or any person who was born outside the jurisdiction of the United States, is a citizen of a foreign country, and has not become a naturalized U.S. citizen under U.S. law. This includes legal permanent residents/lawful permanent residents (LPR), also known as permanent resident aliens, resident alien permit holder, and green card holder. (22 U.S.C. § 6023(8)[[11]](#footnote-12)) and 8 U.S.C. § 1101(a)(3)[[12]](#footnote-13)
12. Incident: An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (OMB Circular A-130)
13. Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (OMB Circular A-130).
14. Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (OMB Circular A-130)
15. Logical Access: Access to a government information system that requires the Contractor (and/or any subcontractor) to logon with a HHS Windows Active Directory account or some other HHS authorized network operating system account. This does not include access to a public web site, whether by an HHS Contractor or member of the public, because such web sites do not require permission to access. In the case of sensitive data/information that exists in hard copy, “access” means providing a contractor the right to view or use written/typed data or information for the purpose described in a contract (HHS Defined).
16. Long-term Access: Access for a period exceeding six months or more than 1,040 hours in any one year (HHS Defined).
17. Non-Public Information: Information that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public. It includes information that he knows or reasonably should know: (a) Is routinely exempt from disclosure under 5 U.S.C. 552 or otherwise protected from disclosure by statute, Executive order or regulation; (b) Is designated as confidential by an agency; or (c) Has not actually been disseminated to the general public and is not authorized to be made available to the public on request (5 CFR 2635.703).
18. Personally Identifiable Information (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 M-17-12).
19. Physical Access: “Physical” entry to and/or exit from a federally controlled facility (HHS Defined).
20. Public Information: Any information, regardless of form or format, that an agency discloses, disseminates, or makes available to the public. (OMB Circular A-130)
21. Requiring Activity: Group or individual responsible for defining the acquisition requirements needed to assist HHS in completing a duty or task. (HHS defined)
22. Routine Access: Access that is on a regular, non-intermittent basis, which is at least once per week during the contract or order period of performance (HHS Defined).
23. Safeguarding: Measures or controls that are prescribed to protect information systems. (FAR 52.204-21)
24. Sensitive Data/Information: Information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the conduct of HHS programs, or the privacy of individuals’ information protected by The Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA). Information technology (IT) security personnel and system owners can equate this definition of sensitive information with data that has a FIPS 199 security impact level of moderate or high for the Confidentiality security objective. This definition of sensitive information is media neutral, applying to information as it appears in either electronic or hardcopy format (HHS Memo - Updated Departmental Standard for the Definition of Sensitive Information).

1. Information created, collected, processed, disseminated, or disposed of by or for the Federal Government. Also referred to as “government information” per the OMB A-130 at https://obamawhitehouse.archives.gov/omb// [↑](#footnote-ref-2)
2. FAR Subpart 2.1 may be found at https://www.acquisition.gov/?q=/browse/far/2 [↑](#footnote-ref-3)
3. HHSAR Subpart 304.13 may be found at http://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/subpart304-13/index.html [↑](#footnote-ref-4)
4. OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005 may be found at https://obamawhitehouse.archives.gov/omb// [↑](#footnote-ref-5)
5. FAR Subpart 4.13 may be found at https://www.acquisition.gov/?q=/browse/far/4 [↑](#footnote-ref-6)
6. FISMA 2014. [↑](#footnote-ref-7)
7. OMB Circular A-130 [↑](#footnote-ref-8)
8. FAR Part 39 (<https://www.acquisition.gov/?q=/browse/far/39>) [↑](#footnote-ref-9)
9. Purchasing of Noncommercial Computer Software and Open Source Licenses (2012) information may be found at http://www.hhs.gov/ocio/policy/purchasing\_noncommercial\_computer\_software.html [↑](#footnote-ref-10)
10. OMB M-04-16, Software Acquisition, July 1, 2004, may be found at https://obamawhitehouse.archives.gov/omb// [↑](#footnote-ref-11)
11. 22 U.S.C. § 6023(8) may be found at http://uscode.house.gov/view.xhtml?req=(title:22%20section:6023%20edition:prelim [↑](#footnote-ref-12)
12. 8 U.S.C. § 1101(a)(3) may be found at https://www.gpo.gov/fdsys/granule/USCODE-2011-title8/USCODE-2011-title8-chap12-subchapI-sec1101 [↑](#footnote-ref-13)