LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Security and Privacy Language for Information and Information Technology Procurements

Version 2.0

June 26, 2017

Table of Contents

procurements

Document Change History

Version Number	Date	Section/Page Number	Summary of Changes	Author
1.0	May 2012	General	Initial release of *Security and Privacy Guide for Information Technology Acquisition*	OCIO
2.0	June 2017	General	The document has been reformatted to include the standard baseline security and privacy contract language to be used across the Department as well as procedures, guidance and instructions to apply the standard language.	OCIO/OIS/GRC

1. Introduction

The Department of Health and Human Services (HHS) is responsible for implementing and administering an information security program to protect its information resources in compliance with applicable public laws, federal regulations, and Executive Orders. This includes the *Federal Information Security Modernization Act (FISMA) of 2014*[1]and Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2]. To meet these requirements, the Department has issued the HHS *Information Security and Privacy Policy (IS2P)*[3], which contains the policies to secure information and information systems throughout the Department.

While the IS2P is the overarching policy governing information technology security and privacy at HHS, it does not provide explicit guidance for the Contracting Officer (CO), Contracting Officer Representative (COR), requiring activity representative[4], and other staff involved in the procurement of information and information technology (IT) products and services. Therefore, the *HHS Security and Privacy Language for Information and Information Technology Procurements* document 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.

This document supersedes the following documents:

- Security and Privacy Guide for Information Technology Acquisition, dated May 15, 2012; and
- Standard for Security Configurations Language in HHS Contracts, dated January 14, 2009.

This is a living document and will be updated as federal laws, regulations, and other guidance change.

A. Purpose

The *HHS Security and Privacy Language for Information and Information Technology Procurements* standard, which aligns with the *Federal Acquisition Regulation (FAR)*[5], the HHS *Acquisition Regulation (HHSAR)*,[6] and other federal and HHS policies, is designed to assist COs, CORs, Program Managers (PMs), and other stakeholders in selecting the appropriate security and privacy language to include in acquisition documents (solicitations, contracts, etc.) for information and IT products and services procurements during pre-award and post-award of a contract. This document provides current information

[1] Public law 113-283, Title 44, United States Code, Federal information Security Modernization Act of 2014 (FISMA) may be found at https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf (44 U.S.C. 101)
[2] OMB A-130,Managing Information as a Strategic Resource, July 28, 2016 may be found at https://obamawhitehouse.archives.gov/omb//
[3] The HHS IS2P is retrievable from https://intranet.hhs.gov/it/cybersecurity/policies/index.html
[4] Requiring activity is often referenced in the FAR and refers to the entity acquiring goods and/or services. See the Federal Acquisition Regulation (FAR), retrievable from: http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title48/48tab_02.tpl.
[5] Ibid.
[6] HHS Acquisition Regulation (HHSAR), retrievable from: https://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/index.html

security and privacy requirements to ensure federally-mandated security and privacy controls and standards are met within the Department. Operating Divisions (OpDivs) may customize this document to include OpDiv specific information or create their own document or suplement the standard contract language, provided the OpDiv contract language is compliant with and as restrictive as the baseline contract language stated herein.

Additional references are included in Appendix H for ease of use.

B. Background

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. In accordance with OMB memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*[7], and FAR subpart 7.1, *Acquisition Plan*, agency heads must ensure all agency personnel involved with IT procurements understand how to meet FISMA guidance and standards set forth in OMB Circular A-130 and the National Institute of Standards and Technology (NIST) guidelines[8]. In addition, the Federal Information Technology Acquisition Reform Act (FITARA)[9], enacted in 2014, mandates that government agencies' chief information officers (CIOs) have a significant role in IT procurements decisions and oversight.

C. Scope

As prescribed by the HHS Deputy Secretary's "FY15 Cybersecurity Information Technology (IT) Priorities", Action 2, this document contains standardized security and privacy language to be used in solicitations and contracts when acquiring information and information technology.[10] This document supplements federal and HHS acquisition guidance (See Appendix H - References). Only the Office of the Assistant Secretary for Financial Resources (ASFR)/Office of Grants and Acquisition Policy and Accountability (OGAPA) Division of Acquisition (DA), in conjunction with Office of the Chief Information Officer (OCIO), may issue HHS acquisition policy.

In addition, designated health care components (for simplicity hereinafter referred to as covered components) within HHS that are subject to the regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA)[11] and the Health Information Technology for Economic and Clinical Health (HITECH) Act[12] 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 shall impose a duty to cooperate with the covered component and/or the Department's breach investigation and response, and shall 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 a health care

---

[7] OMB M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006 may be found at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-20.pdf
[8] NIST guidelines may be found at http://csrc.nist.gov/publications/
[9] FITARA may be found at https://www.congress.gov/bill/113th-congress/house-bill/1232.
[10] DepSec FY15 Priorities may be found at http://intranet.hhs.gov/it/cybersecurity/policies/index.html
[11] HIPAA may be located at https://www.hhs.gov/hipaa/for-professionals/index.html.
[12] HITECH Act may be located at https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

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 health care that uses electronic transactions. More information about requirements for business associates and sample contract language can be found on the Office for Civil Rights (OCR) Website.[13]

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/or the Chief Information Security Officer (CISO), are responsible for ensuring the acquisition documentation includes the appropriate information security and privacy requirements and sufficient details to enable Contractors and service providers to fully understand the information 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. 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. 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;
- Procurements involving cloud services;
- Other procurement types
    - Hardware,
    - Non-commercial and open source software,
    - Information technology application design, development or support, and
    - Physical access to government controlled facilities only.

D. Applicability

The security and privacy requirements set forth herein apply to all new and existing information and IT solicitations and contracts, irrespective of dollar amount. To determine the applicable language for each solicitation and contract, the requiring activity representative must confer with their OpDiv's Information System Security Officer (ISSO)/Chief Information Security Officer (CISO) and Privacy Officer/Senior Official for Privacy (SOP) to complete the "Information Security & Privacy Certification Checklists" in Appendix A. All procurements for IT and information services must complete this security and privacy review.

*Use the information from the completed Checklist to populate the missing information in **subsection 3 Information Security Categorization** in the standard language in **Section 2**.*

In addition, see Appendix F for list of security and privacy points of contact and Appendix E for guidance in determining applicable security and privacy language.

[13] OCR website may be located at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentties/businessassociates.html.

The standard security and privacy language stated herein may apply to procurements that are subject to HIPAA and HITECH.[14]

The standard security and privacy language stated herein is not intended for agreements that are not subject to the FAR, such as grants and cooperative agreements[15]. Drafters of those types of agreements may need to consult the applicable agency personnel to ensure their agreements, and grantees, are compliant with all applicable federal security and privacy requirements.

The standard security and privacy language stated herein applies to FISMA systems and does not apply to national security systems. Additional information may be found on the HHS Classified National Security Information Policy[16].

E. Effective Date/Implementation

The effective date of this document is the date the document is approved. OpDivs shall begin the implementation of the standard security and privacy language stated herein within ***ninety (90) days*** of document issuance date.

[14] Additional information about HIPAA acquisition requirements may be found on the OCR Website at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.
[15] Additional information on grants and cooperative agreements may be found on the HHS Contract and Grants Support Website at: https://intranet.hhs.gov/abouthhs/contracts-grants-support/index.html.
[16] The HHS Classified National Security Information Policy may be found at: https://intranet.hhs.gov/security/ossi/documents/cnsi.pdf.

F. Approved

/S/ 6-26-2017

Beth Anne Killoran DATE
HHS Chief Information Officer

/S/ 6-6-2017

Andrea L. Brandon, MPA DATE
Deputy Assistant Secretary
Office of Grants and Acquisition Policy and Accountability

2. 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[17] 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.[18]

Physical and Logical Access refers to when contractor personnel (and/or any subcontractor) are expected to have (1) routine physical access to an HHS-controlled facility; (2) logical access to an HHS-controlled information system; (3) access to government information, whether in an HHS-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[19] and OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* [20].

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 HHS-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 OpDiv 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[21], 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.)

[17] 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//
[18] FAR Subpart 2.1 may be found at https://www.acquisition.gov/?q=/browse/far/2
[19] HHSAR Subpart 304.13 may be found at http://www.hhs.gov/grants/contracts/contract-policies-regulations/hhsar/subpart304-13/index.html
[20] 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//
[21] FAR Subpart 4.13 may be found at https://www.acquisition.gov/?q=/browse/far/4

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 OpDiv's CISO or designee to complete the checklist in Appendix A (Part A and Part B) to determine OpDiv-specific requirements, and identify any additional security language applicable to the solicitation/contract. See Appendix F for list of security points of contact.

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.

Replace ALL bracketed wording with YOUR OPDIV'S SPECIFIC REQUIREMENT.

1) Copy language from "Start Copying Language Below" to "Stop Copying Language Here".
2) Perform a global search for ***[OpDiv…]*** and replace with appropriate text.

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

A. Baseline Security Requirements

1) **Applicability.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

   a. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information.

   b. 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.** In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:

a. Protect government information and information systems in order to ensure:
   - **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.

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, **within one (1) hour or less**, bring the situation to the attention of the other party.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS 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 the HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

d. Comply with the Privacy Act requirements and tailor FAR clauses as needed..

3) **Information Security Categorization**. 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 Categorie*s, Appendix C, and based on information provided by the ISSO, CISO, or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality:	[ ] Low [ ] Moderate [ ] High
Integrity:	[ ] Low [ ] Moderate [ ] High
Availability:	[ ] Low [ ] Moderate [ ] High
Overall Risk Level:	[ ] Low [ ] Moderate [ ] High

Based on information provided by the ISSO, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [ ] Yes PII

Complete this section using the information obtained from the Security and Privacy Checklist in Appendix A, parts A and B.

Personally Identifiable Information (PII). Per the Office of Management and Budget (OMB) Circular A-130, "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.

PII Confidentiality Impact Level has been determined to be: [ ] Low [ ] Moderate [ ] High

4) **Controlled Unclassified Information (CUI).** CUI is defined 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 "h*andling"* 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. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

   a. marked appropriately;

   b. disclosed to authorized personnel on a Need-To-Know basis;

   c. protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Federal 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

   d. returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

5) **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) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

See the HHS Standard for the Definition of Sensitive Information, for additional information in defining and protecting sensitive information.

6) **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 shall be used only for the purpose of carrying out the provisions of this contract and shall 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 shall ensure that all work performed by its employees and subcontractors shall 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 shall 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 shall be protected in accordance with HHS and *[OpDiv]* policies. Unauthorized disclosure of information will be subject to the HHS/*[OpDiv]* sanction policies and/or governed by the following laws and regulations:

a. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
b. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
c. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

7) **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*. .

8) **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 shall 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, the HTTPS is not required, but it is highly recommended.

9) **Contract Documentation**. The Contractor shall use provided templates, policies, forms and other agency documents *[OpDiv specify which documents/forms will be provided to contractor]* to comply with contract deliverables as appropriate.

*See **Appendix D** for baseline deliverables.*

10) **Standard for Encryption.** The Contractor (and/or any subcontractor) shall:

a. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.

b. 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 FIPS 140-2 validated encryption solution.

c. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OpDiv-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).

d. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR *[OpDiv-provided delivery date]*.

e. 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. Encryption keys shall be provided to the COR upon request and at the conclusion of the contract.

11) **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the OpDiv non-disclosure agreement. *[OpDiv inserted information/link should be cited here]*, as applicable. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

See Appendix C for the HHS Contractor Non-Disclosure Agreement.

12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the OpDiv Senior Official for Privacy (SOP) or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist the OpDiv SOP or designee with completing a PIA for the system or information within *[OpDiv 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*.

b. The Contractor shall assist the OpDiv SOP or designee 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.

B. Training

1) **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable HHS/OpDiv Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete *[OpDiv-specified]* Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training shall 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) shall maintain training records for all its employees working under this contract in accordance with HHS policy. A copy of the training records shall be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

C. Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, and [*insert any OpDiv-specific rules, as applicable*].

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 OpDiv 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.

D. Incident Response

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/*[OpDiv]* IRT 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.. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by Federal Information Security Modernization Act (FISMA) as 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. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines a breach as "a suspected or confirmed incident involving PII" .

In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1) Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as to avoid a secondary sensitive information incident with FIPS 140-2 validated encryption.

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 shall

send *[OpDiv]* approved notifications to affected individuals [*insert OpDiv Specific timeline, process, and format]*.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the OpDiv Incident Response Team (IRT) *[OpDiv inserted contact information should be cited here]*, COR, CO, OpDiv SOP (or his or her designee), and other stakeholders, including incidents 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 OpDiv 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, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

   a. cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;

   b. not include any sensitive information in the subject or body of any reporting e-mail; and

   c. 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* HHS/OpDivHHS and*[OpDiv]* incident 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 *[OpDiv insert timeline if required]*.

E. 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:

> *The requiring activity representative, in conjunction with Personnel Security, shall use the OPM Position Sensitivity Designation automated tool (https://www.opm.gov/investigations/) to determine the sensitivity designation for background investigations. After making those determinations, include all applicable position sensitivity designations.*

F. Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2.*

.

For additional information, see HSPD-12 policy at: https://www.dhs.gov/homeland-security-presidential-directive-12)

Roster. The Contractor (and/or any subcontractor) shall 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 shall be submitted to the COR and/or CO within *[OpDiv Specific timeline]* of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within *[OpDiv Specific timeline]* of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. *[If the OpDiv has an electronic template, include that information here along with a link, if applicable.]*

If the employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate suitability level.

G. Contract Initiation and Expiration

1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall 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 shall follow the HHS EPLC framework and methodology or *[insert OpDiv-specific requirement]* and in accordance with the HHS Contract Closeout Guide (2012).

HHS EA requirements may be located here:
https://www.hhs.gov/ocio/ea/documents/proplans.html

2) **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC 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) shall provide all required documentation *[enter OpDiv-specific requirements]* 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) shall notify the CO and/or COR and system ISSO within *[OpDiv-specific timeline]* before an employee stops working under this contract.

5) **Contractor Responsibilities Upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) shall 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 shall 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 *[OpDiv]* policies.

6) The Contractor (and/or any subcontractor) shall perform and document the actions identified in the ***[OpDiv]*** Contractor Employee Separation Checklist *[insert links to OpDiv form]* when an employee terminates work under this contract within *[insert OpDiv-specific timeline]* days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. Records Management and Retention

The Contractor (and/or any subcontractor) shall 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/*[OpDiv]* policies and shall not dispose of any records unless authorized by HHS/*[OpDiv]*.

In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, it shall be documented and reported as an incident in accordance with HHS/*[OpDiv]* policies.

STOP COPYING LANGUAGE HERE

3. 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/OpDiv Senior Official for Privacy (SOP) who completes Appendix A must consult with the System/Data Owner and the OpDiv 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 OpDiv-specific System of Records Notices (SORNs) that cover the records, or to confirm if a new or revised SORN is needed. Privacy Act Contacts are listed in Appendix F. 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

A. 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 on individuals. .

The System of Records Notice (SORN) that is applicable to this contract is: *[OpDiv insert SORN number if one exists. If there is no SORN, indicate that a SORN will be developed]*.

The design, development, or operation work the Contractor is to perform is: *[OpDiv 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: *[OpDiv insert records disposition instructions the contractor and any subcontractor must follow upon completion of contract performance]*.

STOP COPYING LANGUAGE HERE

4. Procurements Involving Government Information Processed on GOCO or COCO Systems

DIRECTIONS

The Federal Information Security Modernization Act (FISMA of 2014, (44 U.S.C. 101)[22], Office of Management and Budget (OMB Circular A-130, *Managing Information as a Strategic Resource*[23], and Federal Procurements Regulation (FAR) 39.101[24] 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 followingdefinitions 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 OpDiv 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. OpDivs should strive to have contractors obtain independent third party verification, but can accept contractor or government certifications, based on its 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.**

Replace ALL bracketed wording with YOUR OPDIV'S SPECIFIC REQUIREMENT(S).

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

[22] FISMA 2014.
[23] OMB Circular A-130
[24] FAR Part 39 (https://www.acquisition.gov/?q=/browse/far/39)

contract.

START COPYING LANGUAGE BELOW

A. Security Requirements for GOCO and COCO Resources

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy (IS2P), [enter applicable OpDiv policy if any]*; *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, *Security and Privacy Controls for Federal 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) **Security Assessment and Authorization (SA&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) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) *[OpDiv enter timeline(s)]*. The Contractor shall conduct the SA&A requirements in accordance with *HHS IS2P/ [Insert OpDiv policy if any]*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

For an existing ATO, OpDiv must make a determination if the existing ATO provides appropriate safeguards or *if an additional ATO is required for the performance of the contract and state as such.*

[Insert OpDiv here] acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

a. SA&A Package Deliverables - The Contractor (and/or any subcontractor) shall provide an SA&A package within *[OpDiv include timeline, process, and format for SA&A package delivery or indicate timeline/format for each individual deliverable]* to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package *[insert OpDiv-specific deliverables (if any) in addition to the HHS baseline listed below]*:

- **System Security Plan (SSP)** – due *[insert specific timeline, process, and format after contract award]*. The SSP shall 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 Federal 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 *[OpDiv]* policies and other guidance. The SSP shall 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 shall 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 shall update the SSP at least ***annually***

thereafter.

- **Security Assessment Plan/Report (SAP/SAR)** – due *[insert specific timeline, process and format after contract award.]* The security assessment shall be conducted by *[OpDiv include type of assessment]* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

  The OpDiv should determine which security control baseline applies and then make a determination on the appropriateness/necessity of obtaining an independent assessment. Assessments of controls can be performed by contractor, government, or third parties, with third party verification considered the strongest. If independent assessment is required, include statement below.

  Thereafter, the Contractor, in coordination with ***[****OpDiv****]*** shall *[conduct/assist]* in the assessment of the security controls *[insert specific timeline(s) if applicable*] and update the SAR at least ***annually***.

- **Independent Assessment -** due *[insert specific timeline, process, and format after contract award]*. The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall 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 shall address all *"high"* deficiencies *[OpDiv enter all other deficiencies required to be mitigated by Contractor]* before submitting the package to the Government for acceptance. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).

- **POA&M** – due *[insert specific timeline, process, and format after contract award]*. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. All high-risk weaknesses must be mitigated within *[insert specific timeline]* and all medium weaknesses must be mitigated within *[insert specific timeline]* from the date the weaknesses are formally identified and documented. *[OpDiv]* will determine the risk rating of vulnerabilities.

  Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, ***[****OpDiv****]*** may require designated POAM weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least ***quarterly*** *[insert timeline, process, and format if more frequent updates are needed]*.

- **Contingency Plan and Contingency Plan Test** – due *[insert specific timeline, process and format after contract award]*. 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 OpDiv policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall 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 shall update and test the Contingency Plan at least ***annually***.

- **E-Authentication Questionnaire** – The contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (E-auth TA) is completed to determine if a full E-Authentication Risk Assessment (E-auth RA) is necessary. System documentation developed for a system using E-auth TA/E-auth RA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

  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 policies.

b. 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, shall 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*, and HHS IS2P. The following are the minimum requirements for ISCM:

- **Annual Assessment/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 may involve penetration testing conducted by the agency or independent third-party *[insert OpDiv pen test requirement if needed]*.) In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date *[OpDiv provided]*.

- **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-owned information/data. It is anticipated that this inventory information will be required to be produced at least *[insert specific timeframe]*. IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

- **Configuration Management** - Use available SCAP-compliant automated tools, per NIST IR 7511, for authenticated scans to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, application, etc.) that store and process government information. Compliance will be measured using IT assets and standard HHS and government configuration baselines at least *[insert specific timeframe]*. The contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

- **Vulnerability Management -** Use SCAP-compliant automated tools for authenticated

scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall 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 *[insert specific timeframe]*.

- **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 agency specified timeframes *[insert specific timeframe]*.

- **Secure Coding** - Follow 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.

- **Boundary Protection** - The contractor shall 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) shall 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, including but are not limited to:

   a. 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.

   b. 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.

c. Segregate Government protected information and metadata on the handling of Government protected information from other 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.

d. 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). The contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS *End-of-Life Operating Systems, Software, and Applications Policy*.

5) **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor**. The Contractor (and/or any subcontractor) shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

a. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-2 encryption standards.

b. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), *[OpDiv insert specific security configuration baseline if any],* and HHS *Minimum Security Configuration Standards*;

c. Maintain the latest operating system patch release and anti-virus software definitions *[insert OpDiv specific timelines]*;

d. 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

e. Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

- Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

- Using Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner 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.

STOP COPYING LANGUAGE HERE

5. 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 OpDiv's System Owner, ISSO or CISO, and OpDiv 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/OpDiv-specific contract clauses to ensure that FedRAMP, HHS, and OpDiv 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. OpDivs 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 OpDiv 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).

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

A. HHS FedRAMP Privacy and Security Requirements

The Contractor (and/or any subcontractor) shall be responsible for the following privacy and security requirements:

1) **FedRAMP Compliant ATO**. Comply with FedRAMP Security Assessment and Authorization (SA&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 shall submit a plan to obtain a FedRAMP compliant ATO by *[insert specific timeframe, process and format for contractor to submit ATO package and/or deliverables]*.

    a. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.
    b. 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 shall store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS) if so required *[OpDiv define locations and boundaries]*.

3) **Service Level Agreements.** *Add when applicable* The Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with *[OpDiv]* to develop and maintain an SLA.

4) **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor shall establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS/*[OpDiv]* policies.

B. 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 shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/*[OpDiv]* policies.

2) HHS will retain unrestricted rights to federal data handled under this contract. Specifically, HHS retains ownership of any user created/loaded data and applications collected, maintained, used, or

operated on behalf of HHS 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 within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data shall be provided at no additional cost to HHS.

3) The Contractor (and/or any subcontractor) shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

4) The contractor shall 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:

   a. Maintenance of links between records and metadata, and

   b. 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 data shall be at the written direction of HHS/*[OpDiv]*. This may include documents returned to HHS control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

6) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements *[OpDiv include Privacy Act language from Section 3]*.

C. Security Assessment and Authorization (SA&A) Process

1) The Contractor (and/or any subcontractor) shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, and HHS policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/*[OpDiv]* security policies *[OpDiv insert language that specifies when the contractor must obtain certification]*.

   a. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation *[OpDiv include additional language needed (depending on the level of effort determined by ISSO, or other relevant stakeholder) and completion/submission timelines]*. The agency ATO must be approved by the *[OpDiv]* authorizing official (AO) prior to implementation of system and/or service being acquired.

   b. 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. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

   c. For all acquired cloud services, the SA&A package must contain the following

documentation *[OpDiv include either the SA&A package deliverables from Section 4 or deliverables mentioned in the FedRAMP Standard Contract Language available on the FedRAMP site]*. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/*[OpDiv]* policies. [*OpDiv must also specify whether the contractor should use the FedRAMP templates (http://www.fedramp.gov/) or OpDiv templates and include specific deliverables timelines*].

2) HHS reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If HHS exercises this right, the Contractor (and/or any subcontractor) shall allow HHS employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with HHS 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.

3) 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, all gaps shall be documented and tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the contractor's expense, before HHS issues an ATO.

4) The Contractor (and/or any subcontractor) shall mitigate security risks for which they are responsible, including those identified during SA&A and continuous monitoring activities. All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery: (1) critical vulnerabilities no later than ***thirty (30) days*** and (2) high, medium and low vulnerabilities no later ***than sixty (60) days****[or shorter timelines provided by OpDiv]***.** In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they shall be added to the designated POA&M and mitigated within the newly designated timelines *[insert OpDiv timelines for mitigating POA&M weaknesses]*. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

5) **Revocation of a Cloud Service**. HHS/*[OpDiv/StaffDiv]* 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 and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or *[OpDiv]* 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.

D. 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. ***[OpDiv***

include meetings/deliverables timelines as applicable/necessary]

OpDiv include all applicable Continuous Monitoring language from Section 4 and approved CSP specific Continuous Monitoring Plan.

2) At a minimum, the Contractor must provide the following artifacts/deliverables on a ***monthly*** basis *[OpDiv insert process and format for deliverables]:*

   a. Operating system, database, Web application, and network vulnerability scan results;
   b. Updated POA&Ms;
   c. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the [OpDiv] System Owner or AO; and
   d. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/[OpDiv]'s 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.

E. Configuration Baseline

1) The contractor shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/OpDiv *[enter OpDiv Specific configuration requirements]* configuration baseline.

2) The contractor shall use Security Content Automation Protocol (SCAP) validated tools with configuration baseline scanner capability to certify their products operate correctly with HHS and NIST defined configurations and do not alter these settings.

F. Incident Reporting

Include Incident Response language from Section 2

1) The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS *[OpDiv]*, OMB, and US-CERT requirements and obtain approval from the OpDiv. 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 access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within ***72 hours*** of notification. The program of inspection shall include, but is not limited to:

   a. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS*/[OpDiv]* personnel, or agents acting on behalf of HHS*/[OpDiv]*, 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.

b. 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.

G. Media Transport

1) The Contractor and its employees shall 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) *[OpDiv include appropriate actions such as logging and a documented chain of custody form]*.

2) All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

H. Boundary Protection: Trusted Internet Connections (TIC)

1) The contractor shall 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.

2) The contractor shall route all external connections through a TIC.

3) **Non-Repudiation.** The contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

STOP COPYING LANGUAGE HERE

6. 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.

The OpDiv 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 OpDiv 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.

A. Hardware Procurements

START COPYING LANGUAGE HERE

1) **Card Readers.** The Contractor (and/or any subcontractor) shall include Federal Information Processing Standard (FIPS) 201-compliant smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops.

2) **Mobile Devices**. The contractor shall follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* when using mobile devices that process or store HHS data.

STOP COPYING LANGUAGE HERE

B. Non-Commercial and Open Source Computer Software Procurements

(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 Guidance

for Purchasing Noncommercial Computer Software and "Open Source" Licenses (2012),[25] and OMB M-04-16, Software Acquisition[26].

If HHS 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

The Contractor (and/or any subcontractor) shall 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.

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

STOP COPYING LANGUAGE HERE

C. Information Technology Application Design, Development, or Support

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

a. 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

b. 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) The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user

[25] 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
[26] OMB M-04-16, Software Acquisition, July 1, 2004, may be found at https://obamawhitehouse.archives.gov/omb//

context without requiring elevated administrative privileges.

2) The Contractor (and/or any subcontractor) shall follow 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.

3) The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS 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 shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data shall be used during software testing.

4) The Contractor (and/or any subcontractor) shall 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 shall 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

D. Physical Access to Government Controlled Facilities

(NOTE: For procurements involving physical access to government facilities, selected language from Section 2 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.)

Appendix A. Information Security Certification Checklist (Internal Use Only)

This security and privacy checklist includes Part A and Part B. Part A should be completed in coordination with the ISSO, System Owner, and/or Program/Project Manager, and signed by the OpDiv Chief Information Security Officer (CISO) or designee. Part B should be completed by the the requiring activity in coordination with the Privacy Officier, Data Owner and/or Program/Project Manager, and signed by the OpDiv Senior Official for Privacy (SOP) or designee. The purpose of this form is to determine if the procurement 1) requires information security, 2) involves personally identifiable information (PII) or 3) is subject to the Privacy Act. This Checklist is for internal use only and will not be included in the package of documents submitted to Contractor. The information obtained with the completion of this checklist will be used to complete **Section 2.A.3**.

The title of document may be changed to meet OpDiv-specific needs. In addition, the OpDiv may include additional information that is pertinent to the acquisition.)

Unique Procurement ID:_____

Pre-Solicitation Review Date: _____

Project Title:_____

Contracting Officer/Contract Specialist: _____
(Name and Contact Information)

Information Technology (IT) Security Representative: _____
(Name and Contact Information)

Senior Official for Privacy or Representative: _____
(Name and Contact Information)

System/Data Owner or Program Manager: _____
(Name and Contact Information)

Information Security Categorization – Part A

PRE-SOLICITATION

[ ] Information security is not applicable. Proceed to the signature page and include this form with the RFP.

[ ] Information security is applicable and the following information is required for RFP preparation:

INFORMATION SECURITY CATEGORIZATION

(NOTE: Categorize the system and/or information and select the appropriate information type(s) below. Then, list the specific element(s) within those information types that are relevant to the acquisition.)

[ ] Information Types: Use the National Institutes 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/) to determine the applicable information type(s). Enter information types in Table 1 below (add/remove rows as needed).

[ ] Mission/Program Based Information: For all selected information types from the NIST 800-60, rate the risk of all information types. The NIST-defined risk ratings may be changed to reflect the actual risk to the agency/program mission. If changing the NIST risk ratings, an explanation for changing the ratings must be included.

[ ] Information/Information System Categorization: Use the Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, (http://csrc.nist.gov/publications/) to categorize the information and/or information system and determine the overall risk. The overall risk is based on the highest water mark (e.g., if Confidentiality is **Moderate**, Integrity is **Low** and Availability is **Low**, the overall rating is **Moderate**.) Enter the overall risk rating in Table 2 below.

Security Categorization Level:

Information Type (Number and Title)	Confidentiality (Low, Moderate, High)	Integrity (Low, Moderate, High)	Availability (Low, Moderate, High)

Table 1: Information Types and Risk Ratings

Information/System Categorization:

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

Table 2: Information/System Categorization and Overall Risk

E-AUTHENTICATION RISK ASSESSMENT

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

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

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

including remote authentication.

Level of Assurance: [ ] N/A [ ] Level 1 [ ] Level 2 [ ] Level 3 [ ] Level 4

Authentication Method: [ ] N/A [ ] Single-Factor [ ] Two-Factor [ ] Multi-Factor

POSITION SENSITIVITY DESIGNATIONS

ISSO, CISO, or representative, in coordination with the requiring activity representative and Personnel Security Offices, determine the applicable position designations using OPM's Position Sensitivity Designation Automated Tool, which is located at: https://www.opm.gov/investigations/. The position sensitivity levels that apply to this solicitation/contract are:

PROSPECTIVE OFFEROR NON-DISCLOSURE AGREEMENT

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

[ ] Offerors **WILL** require access to sensitive information in order to prepare an offer. A Non-Disclosure Agreement (NDA) is necessary for a prospective offeror who will require access to Government information in order to prepare an offer (i.e., a prospective offeror must access an HHS computer room floor plan). *[See Appendix B for Non-Disclosure Agreement form.]*

DESCRIPTION OF SENSITIVE INFORMATION:

Select appropriate position sensitivity designation below.

[ ] Level 6C: Sensitive - High Risk

[ ] Level 5C: Sensitive - Moderate Risk

Information Privacy Certification – Part B

PRE-SOLICITATION

Upon notification from the requiring activity, the HHS/OpDiv Senior Official for Privacy in coordination with the OpDiv Privacy Act Contact or the Departmental Privacy Act Officer shall complete this form to categorize the information collected/handled by this solicitation/contract. The purpose of this form is to categorize the information and determine the privacy requirements and language to be included in this solicitation.

[ ] No privacy requirements apply to this solicitation. Proceed to the signature page.

[ ] Privacy requirements[27] apply to this solicitation. Complete the checklist and sign below.

[27] The E-Government Act of 2002 Section 208 (E-Government Act) and Office of Management and Budget (OMB) Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of 2002, form the core of the Privacy Impact Assessment (PIA) requirement. Together, they state that a PIA is an assessment of how information is handled within certain electronic systems. Each PIA should

[ ] Privacy Act applies to this solicitation. Complete the information below and sign the checklist.

The following tailored information is required for RFP preparation.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

Select the PII Confidentiality Impact Level. For additional information, see NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (http://csrc.nist.gov/publications/PubsSPs.html)**.**

PII[28] Overall Level: [ ] No PII [ ] Yes PII

If yes for PII, insert language from the following sections/sub-sections

- Section 2: All
- Section 3: Applicable language as determined by the OpDiv Senior Official for Privacy

PRIVACY ACT

If Privacy Act requirements apply, complete the following:

TAILORED PRIVACY ACT INFORMATION: Provide the following information if the Privacy Act applies to this solicitation (this is needed to tailor the SOW as required by the HHSAR "Privacy Act" clause, 352.224-70):

- Applicable SORN number(s), or statement that a SORN will be developed:
- Description of design, development, or operation work:
- Records disposition instructions:

PROSPECTIVE OFFEROR NON-DISCLOSURE AGREEMENT

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

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

Appendix B contains the NDA template

consider: 1) Whether the system complies with legal, regulatory, and policy requirements related to privacy; 2) The risks and effects of how that system handles personally identifiable information (PII); and 3) How the system could be changed to mitigate potential privacy risks. The Department of Health and Human Service (HHS) has chosen to evaluate the privacy implications of all electronic systems regardless of whether the E-Government Act or OMB M-03-22 requires a PIA.

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

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

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

Printed Name: _____ Date: _____

OpDiv Senior Privacy Official (SOP) or Representative Signature: _____

Printed Name: _____ Date: _____

Program Manager Signature: _____

Printed Name: _____ Date: _____

Appendix B. Prospective Offeror Non-Disclosure Agreement (NDA)

(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 OpDiv may modify this NDA to accommodate additional agency/contract requirements.

Information and Information Technology Systems Security Non-Disclosure Agreement (NDA)
Request For Proposal (RFP) No: _____
(Fill in the RFP Number)

Project Title: _____
(Fill in Title from RFP)

_____(*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 RFP 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 *[OpDiv, 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

Appendix C. Contractor Non-Disclosure Agreement

This NDA is to be completed by a contractor upon award of contract.

This is a baseline template and the OpDiv may modify the NDA to accommodate additional agency/contract requirements.

Information Technology Systems Security Contractor Non-Disclosure Agreement

Access to sensitive information (such as personally identifiable information [PII]), non-public information, confidential information, and/or Controlled Unclassified Information (CUI) from the files of the Department of Health and Human Services (HHS) is required in the performance of my official duties, under contract number__between (HHS I/C Name or Component)_____ _____and my employer (Employer's Name) _____. I agree that I shall not release, publish, or disclose such information to unauthorized personnel, and I shall protect such information in accordance with relevant federal laws, regulations, and guidelines. *[OpDiv, insert applicable laws if any.]*

I affirm that I have received a written and/or verbal briefing by my company concerning my responsibilities under this agreement. I understand that violation of this agreement may subject me to criminal and civil penalties.

Signed: _____

Type or Print Name: _____

Date: _____

Witnessed by: _____

Date: _____

Copies are to be retained by: HHS Contracting Officer Representative
Contractor's Contract Management
Individual Signatory

Appendix D. 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 *[OpDiv 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	Within *[OpDiv-specific timeline]* of the effective date of this contract	
2 – Contractor Employee Non-Disclosure Agreement (NDA)	Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS	
2 – Privacy Threshold Analysis (PTA)/ Privacy Impact Assessment (PIA)	Assist in the completion of a PTA/PIA form	Within *[OpDiv insert contract-specific timeline]* 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 government	
2 – Personnel Security Responsibilities	List of Personnel with defined roles and responsibilities	Within *[OpDiv-specific timeline]* that is before an employee begins working on this contract.	
2 – Personnel Security Responsibilities	Off-boarding documentation, equipment and badge when leaving contract	Within *[OpDiv-specific timeline]* after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.	
2 – Background Investigation	Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS	
2 - Certification of Sanitization of Government and Government Activity-	Form or deliverables required by OpDiv.	At contract expiration. *[OpDiv-specific]*	

Document Section	Deliverable Title/Description	Due Date	Applicable (y/n)
Related Files, Information, and Devices.			
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. *[OpDiv-specific]*	
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 OpDiv-specific documents	Due within *[insert contract-specific timeline]* after contract award.	
5 – Protection of Information in a Cloud Environment	Contract expiration	Due within *[insert contract-specific timeline]* 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 OpDiv-specific documents	Due within *[insert contract-specific timeline]* after contract award.	
5 – Reporting and	POA&M updates;	Monthly/as requested by	

Document Section	Deliverable Title/Description	Due Date	Applicable (y/n)
Continuous Monitoring	Revised security documentation/Agreements	OpDiv	
5 – Security Alerts, Advisories, and Directives	List of personnel with designated roles and responsibilities	OpDiv-Specified	
5 – Incident Reporting	• Incident reports (as needed) • Incident Response Plan	OpDiv-Specified	
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 HHS	

Appendix E. Decision Tree Table

The following decision table has been created to assist Procurement/Program personnel in determining the standard security/privacy language that needs to be included in their acquisition documentation (solicitation, Statement of Work [SOW], Statement of Objectives [SOO] or Performance Work Statement [PWS]) as well as applicable FAR and HHSAR clauses that need to be included in Section I of the Contract.

NOTE: The decision criteria below are only a guide and may not be sufficient to determine the standard security/privacy language that applies to your procurement. You must consult with your OpDiv Security/Privacy points of contact (POCs) to identify the applicable security/privacy language, requirements, and/or deliverables.

Criteria Question – Does your acquisition…	**If yes, insert language from the following sections/sub-sections**	**HHSAR/FAR Clauses**	**Complete? (√)**
require routine physical and logical access to controlled government facilities and systems?	• Section 2: All • Section 3: applicable language as determined by the OpDiv Senior Official for Privacy	Examples of applicable clauses: FAR 52.204-9 Personal Identity Verification of Contractor Personnel FAR 52.239-1 Privacy or Security Safeguards, etc.	
require routine physical access to controlled government facilities?	• Section 2: applicable language may include: Training, Incident Response, HSPD-12, and from Baseline Security Requirements no. 9 and 10		
require physical and logical access to government systems and/or data housed at Contractor facilities?	• Section 2: All • Section 3: applicable language as determined by the OpDiv Senior Official for Privacy Section 4: All	FAR 52.239-1 Privacy or Security Safeguards; FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems; etc.	

Criteria Question – Does your acquisition…	**If yes, insert language from the following sections/sub-sections**	**HHSAR/FAR Clauses**	**Complete? (√)**
requires that the contractor or a subcontractor at any tier will have Federal contract information residing in or transiting through its information system?	• Section 2: applicable language as determined by the OpDiv Senior Official for Privacy • Section 3: applicable language as determined by the OpDiv Senior Official for Privacy	FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016); etc.	
involve only logical access to government/contractor owned contractor operated system housing government data?	• Section 2: All • Section 3: applicable language as determined by the OpDiv Senior Official for Privacy • Section 4: All	FAR 52.239-1 Privacy or Security Safeguards; FAR 52.204-21 Basic Safeguarding of Covered Contractor Information Systems; etc.	
involve a cloud service?	• Section 2: All • Section 3: applicable language as determined by the Senior Official for Privacy • Section 4: applicable language as determined by the ISSO • Section 5: All	FAR 52.227-1 Authorization and Consent; FAR 24.104 Contract Clauses; etc.	
involve handling of sensitive information (i.e., PII, PHI, etc.)?	• Section 2: All • Section 3: applicable language as determined by the Senior Official for Privacy • Section 4: applicable language as determined by the ISSO	FAR 52.239-1 Privacy or Security Safeguards; HHSAR 352.224-71 Confidential Information; etc.	
involve a system of records?	• Section 2: All • Section 3: All • Section 4: Include applicable language	FAR 52.239-1 Privacy or Security Safeguards, FAR 24.103 Procedures; etc.	

Criteria Question – Does your acquisition…	**If yes, insert language from the following sections/sub-sections**	**HHSAR/FAR Clauses**	**Complete? (√)**
involve only computer hardware or mobile devices?	• Section 6: Hardware Acquisition	FAR 39 Acquisition of Information Technology, FAR 4.13 Personal Identity Verification; etc.	
involve only software design or support?	• Section 6: Information Technology Application Design or Support	To Be Determined (TBD)	
involve open source software?	• Section 6: Non-Commercial and Open Source Computer Software	TBD	

Appendix F. Points Of Contact Listing

HHS Security & Privacy Points of Contact

HHS/OpDiv	URL
Security Points of Contacts	https://intranet.hhs.gov/it/cybersecurity/ciso/index.html
Privacy Act Points of Contacts	https://intranet.hhs.gov/it/cybersecurity/privacy/index.html
Department Privacy Contacts	http://intranet.hhs.gov/it/cybersecurity/privacy/index.html

HHS Incident Response Points of Contact

CISIRC	**Email: csirc@hhs.gov**
OpDiv	Email
ITO	hhsitio-irt@hhs.gov
AHRQ	CSIRT@ahrq.hhs.gov
ACF	gary.cochran@acf.hhs.gov
ACL	csirt@acl.hhs.gov
SAMHSA	infosecurity@samhsa.hhs.gov
CMS	SOC@cms.hhs.gov
FDA	csirt@fda.hhs.gov
CDC/ATSDR	CSIRT@cdc.gov
IHS	IRT@ihs.gov
NIH	CSIRT@nih.hhs.gov
OIG	csirt@oig.hhs.gov
HRSA	csirt@hrsa.hhs.gov

Appendix G. Roles and Responsibilities

The following is a compilation of the roles and responsibilities for relevant personnel identified in this document.

1. Chief Information Security Officer (CIO)

The CIO is responsible for the following:

- Ensure standard contract security and privacy language is developed, maintained current, and disseminated throughout the Department.
- Ensure IT and information procurements include relevant security and privacy language to protect all HHS systems and information.
- Coordinate with the Office of the Assistant Secretary for Financial Resources (ASFR)/Office of Grants and Acquisition Policy and Accountability (OGAPA's) Division of Acquisition (DA) to ensure all HHS IT contracts are reviewed on a periodic basis to ensure the security and privacy language is current and relevant.

2. Chief Information Security Officer (CISO)

The CISO is responsible for the following:

- Develop and disseminate throughout the Department standard contract security and privacy language.
- Ensure IT and information contracts and other applicable procurements documents include relevant security and privacy language to protect the confidentiality, integrity and availability of HHS systems and information.
- Collaborate with the Office of the Assistant Secretary for Financial Resources (ASFR)/Office of Grants and Acquisition Policy and Accountability (OGAPA's) Division of Acquisition (DA) to ensure all HHS IT contracts are reviewed on a periodic basis to ensure the security and privacy language is current and relevant.
- Approve any deviations from HHS policies and standards.
- Approve the Information Security Solicitation Certification Checklist (Appendix A).
- Ensure the system and information are categorized in accordance with FIPS 199 and NIST 800-60 and HHS level of risk.

3. Information Systems Security Officer (ISSO)

The ISSO is responsible for the following:

- Document any deviations from HHS policies and standards.
- Complete/approve the Information Security Solicitation Certification Checklist (Appendix A).
- Ensure the system and information under Contract are categorized in accordance with FIPS 199 and NIST 800-60 and HHS level of risk.

4. Contracting Officer (CO)

The CO is responsible for the following:

- Coordinate with the Office of the CIO to ensure contract security and privacy language is current and relevant and included in all contracts.
- Coordinate with OSSI to ensure HSPD-12 requirements are included in all contracts.
- Communicate validity decisions from the HHS PIRT to the Contractor.
- Communicate solicitation/contract requirements/issues to/from Contractor.
- Consent to closure activities on the contract (including any disposition of data).
- Provide written permission (if applicable) for HHS to have government purpose rights in software developed with mixed funding.

- Confer with the System Owner, Information System Security Office (ISSO) and/or OpDiv 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.

5. Contacting Officer Representative (COR)

The COR is responsible for the following:

- Assist the CO with the inclusion of relevant security and privacy language in all IT and information acquisition contracts.
- Notify the Contractor of the appropriate level of investigation required for each staff member.
- Communicate incident information, including PII/PHI breaches, from the Contractor to appropriate personnel.

6. Program Manager (PM)

The PM is responsible for the following:

- Review and approve the Information Security Solicitation Certification Checklist (Appendix A).
- Determine which contractor employees have to complete role-based training commensurate with their role and responsibilities.

7. Requiring Activity Representative

The Requiring Activity Representative is responsible for the following:

- Confer with ISSO and System Owner and/or the OpDiv's CISO in the completion of Appendix A.
- Collaborate with the Contracting Officer, Privacy Officer, System Owner, ISSO and/or OpDiv CISO to determine applicable security and privacy language for solicitation/contract, level of access and other contract requirements.

8. OpDiv Senior Official for Privacy (SOP)

The OpDiv SOP is responsible for the following:

- Approve the Privacy Solicitation Certification Checklist (Appendix A).
- Assist in determining the Privacy Act requirements applicable to solicitation/contract.
- Collaborate with ISSO, PM, CO, and or COR to categorize the system of records and/or PII.

9. System Owner

The System Owner is responsible for the following:

- Provide information to help determine the PII confidentiality impact level.
- Complete the Information Security Solicitation Certification Checklist (Appendix A) to categorize the information and/or information system.

10. Contractor/subcontractor

The Contractor (and/or any subcontractor) is/are responsible for the following:

- Protect the Confidentiality, Integrity, and Availability of all government information and information systems.
- Adhere to the terms and conditions specified in Contract, SOW, etc.
- Adhere and comply with agency security and privacy policies, standards, procedures.
- Comply with federal laws, regulations, policies and standards.
- Implement security and privacy requirements specified in Contract, SOW, etc.
- Complete, review, update and submit all deliverables specified in Contract, SOW, etc. by specified due dates.
- Report all suspected and confirmed security and privacy incidents to the COR and other designated personnel.

Appendix H. References (for Internal Staff Use)

NOTE: The title of documents may have changed. Please refer to the most current version and update accordingly when including the standard language in your documentation.

1. Federal 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 M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

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

OMB M-07-17, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, Attachment I.A.2.d.

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

OMB Memo M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

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

OMB M-06-16, *Protection of Sensitive Agency Information.*

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

OMB M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

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.

2. 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).

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/).

3. NIST Guidance (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, *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, *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, Rev. 2 *Electronic Authentication Guideline*, as amended .

NIST SP 800-61, *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, *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.

Appendix I. 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

Appendix J. 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)[29]) and 8 U.S.C. § 1101(a)(3)[30]

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

[29] 22 U.S.C. § 6023(8) may be found at http://uscode.house.gov/view.xhtml?req=(title:22%20section:6023%20edition:prelim
[30] 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

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).