DEPARTMENT OF HEALTH & HUMAN SERVICES Office of the Secretary
Washington, D.C. 20201

HHSAR Class Deviation 2024-01
Amendment 1

MEMORANDUM TO: Heads of the Contracting Activities

FROM: H. Katrina Brisbon katrina brisbon (Mar 1, 2024 12:57 EST)
Deputy Assistant Secretary for the Office of Acquisitions
Senior Procurement Executive

SUBJECT: Amendment 1 to Department of Health and Human Services Acquisition Regulation (HHSAR) Class Deviation (2024-01) from Part 339, Acquisition of Information Technology; Other Parts; Supply Chain Risk Management

EFFECTIVE DATE: March 1, 2024

EXPIRATION DATE: This class deviation is effective until either incorporated into the HHSAR or otherwise rescinded.

PURPOSE: This HHSAR class deviation implements urgent requirements for information, information technology, information security, privacy, security, and supply chain risk management. It removes outdated and redundant policy, aligns the HHSAR with the Federal Acquisition Regulation (FAR), and adds new requirements in HHS acquisitions to identify, assess, and mitigate risks to HHS mission-critical products, materials, information, and services within the supply chain.

Amendment 1 to HHSAR Class Deviation 2024-01 makes corrections and other administrative changes. HHSAR Class Deviation 2024-01, signed on January 24, 2024, is hereby rescinded, and superseded by this Amendment.

DEVIATION: This class deviation revises existing language, removes outdated or redundant coverage, and adds new language concerning the above areas in the following parts (*see* Summary of HHSAR Changes below):

- HHSAR Part 302, Definitions of Words and Terms
- HHSAR Part 304, Administrative Matters
- HHSAR Part 324, Protection of Privacy and Freedom of Information
- HHSAR Part 339, Acquisition of Information Technology
- HHSAR Part 352, Solicitation Provisions and Contract Clauses

BACKGROUND: This class deviation is necessary for the purpose of immediately implementing policy in the HHSAR to comply with requirements of the Federal Information Security Modernization Act and applicable Executive Orders, OMB Memorandums, and other requirements such as National Institute of Standards and Technology (NIST) standards**.** Currently, requirements for information, information technology, information security, privacy, security, and supply chain risk management have been implemented throughout the HHS acquisition enterprise including Operating Divisions and Staff Divisions based on an internally published HHS IT Policy for Security and Privacy for Information and Information Technology Procurements. This important internal policy was necessary to ensure HHS acquisitions included critical requirements in applicable solicitations and contracts. However, 41 U.S.C. 1707(a)(1) requires that a procurement policy, regulation, procedure, or form, including an amendment or modification, may not take effect until 60 days after it is published for public comment in the Federal Register if it "(A) relates to the expenditure of appropriated funds; and (B)(i) has a significant effect beyond the internal operating procedures of the agency issuing the policy, regulation, procedure, or form; or (ii) has a significant cost or administrative impact on contractors or offerors." To ensure the safety, security, integrity, and accessibility of HHS information, information systems, and associated information security, privacy, security, and supply chain risk management policy that is already deployed in the department, it is necessary to issue this class deviation in advance of a proposed rule to ensure it is properly and consistently included in HHS solicitations and contracts. It would seriously jeopardize the critical HHS mission if such policy were held in abeyance while a proposed rule was developed, and important public comment and feedback were received and adjudicated. HHS intends on immediately developing a proposed rule for public comment to provide that opportunity after release of this class deviation.

AUTHORITY: This class deviation is issued under the authority of FAR 1.404, Class deviations, and HHSAR 301.401, Deviations, for the purpose of immediately implementing policy in the HHSAR via a class deviation to comply with requirements of the Federal Information Security Modernization Act, HHS Cybersecurity Program, and applicable Executive Orders, OMB Memorandums, and standards as set forth in the deviated language.

APPLICABILITY: This requirement applies to all HHS Operating Divisions and Staff Divisions for applicable solicitations and contracts as set forth in the attached HHSAR deviation language.

ACTION REQUIRED: Contracting officers shall comply with this class deviation to ensure the policy set forth in the attached HHSAR parts, subparts, sections, and subsections is followed, and any prescribed provisions or clauses are inserted in new solicitations issued and resultant contracts awarded on or after the effective date of the deviation. Heads of the contracting activities (HCA) shall ensure this deviation is disseminated to the acquisition workforce and ensure compliance with the requirements in the class deviation.

In the event of a conflict between this Class Deviation and the HHS Policy for Information Technology Procurements – Security and Privacy Language, this Class Deviation takes precedence.

SUMMARY OF HHSAR CHANGES. To implement the requirements, the HHSAR is deviated and revised, as summarized and provided in Attachment 1 as follows:

1. **HHSAR Part 339, Acquisition of Information Technology (DEVIATION)**. The following sections are revised:

    - **339.000, Scope of part.** This is added to provide scope information.

    - **Subpart 339.1, General.** This subpart is revised to update key information and add a new clause prescription.

    - **339.101, Policy.** This section is revised to remove coverage more appropriate to the scope section. New policy is set forth requiring contracting officers and requiring activities to include in solicitations and contracts the requirement to comply with certain HHS directives, policies, and procedures including the HHS Policy for Information Security and Privacy Protection (IS2P) that establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive orders, policies, regulations, standards and guidance for protecting and controlling HHS sensitive information and ensuring that security requirements are included in acquisitions, solicitations, contracts, purchase orders, and task or delivery orders.

    - **339.106, Contract clauses, and 339.106-70 Information technology security and privacy clauses.** New sections add prescriptions for six new clauses.

    - **Subpart 339.2, Information and Communication Technology (ICT).** The existing subpart title is updated, and new sections are added as follows:

    - **339.201, Scope of subpart; and 339.203, Applicability. Section 339.203-70, Solicitation provision and contract clause,** is revised to update the title, and revises the prescriptions, numbering, and titles of two clauses related to ICT.

    - The following sections are removed as internal operating procedures that will be issued as internal policies, procedures, and guidance and reside in a new HHS Acquisition Manual: **339.204, Exceptions; 339.204-1, Approval of exceptions; and 339.205, Section 508 accessibility standards for contracts.**

2. **HHSAR Part 302, Definitions of Words and Terms (DEVIATION).** The following sections are revised:

    - **302.000, Scope of part.** Added to provide context on the use of definitions throughout the HHSAR and those associated with certain parts.

    - **Subpart 302.1, Definitions**. This subpart is revised to update existing definitions and adds fourteen new definitions, revises two definitions, and removes one definition that is redundant to the FAR or contains policy information more appropriate in another HHSAR part.

3. **HHSAR Part 304, Administrative Matters (DEVIATION).** The following sections are revised:

    - **Subpart 304.13, Personal Identify Verification**. Removes one section **304.1330, Policy**, to more appropriately align with the FAR. Adds two sections: **304.1301, Policy**, and **304.1303, Contract clause**, to provide updated policy and a prescription for new clause **352.204-73, Contractor Personnel Security and Agency Access**.

    - **Subpart 304.19, Basic Safeguarding of Covered Contractor Information Systems.** This adds a new subpart to provide policies and procedures for information security and protection of HHS information, information systems, and sensitive information, including controlled unclassified information. This includes new sections **304.1900-70, Scope of subpart**; **304.1901, Definitions; 304.1902, Applicability**; **304.1970, Information security policy—contractor general responsibilities**; and **304.1903, Contract clause**, that prescribes new clause **352.204-71, Information and Information Systems Security**.

    - **Subpart 304.70, Records Management.** This adds a new subpart to implement National Archives and Records Administration (NARA) records policies. This includes new sections **304.7000, Scope of subpart; 304.7001, Applicability; 304.7002, Definition; 304.7003, Policy; and 304.7004, Contract clause,** to provide updated policy and a prescription for new clause **352.204-72, Records Management**.

4. **HHSAR Part 324, Protection of Privacy and Freedom of Information (DEVIATION).** The following sections are revised as shown in Attachment 1:

    - **Subpart 324.1, Protection of Individual Privacy.** This revises the subpart to add three sections, remove two sections, and revise one existing section.

    - Adds sections **324.101, Definitions**; **324.102, General**; and **324.103-70, Protection of privacy—general requirements and procedures related to business associate agreements**.

    - Removes sections **324.103, Procedures for the Privacy Act,** and **324.104, Restrictions on Contractor Access to Government or Third Party Information**.

    - Revises section **324.105, Contract clauses**, to renumber the section to 324.104 to align with the FAR. Two clauses are prescribed: **352.224-70, Notification of System of Records Notice**, and **352.224-71, Confidential Information**.

    - Adds new **Subpart 324.2, Freedom of Information Act**, containing one section **324.203, Policy**, that provides the agency's procedures for FOIA requests.

5. **HHSAR Part 352, Solicitation Provisions and Contract Clauses (DEVIATION).** Adds new clauses, and revises existing clauses and provisions related to HHSAR parts 304, 324, and 339 as set forth in Attachment 1.

ADDITIONAL INFORMATION: Direct any questions or comments regarding this deviation to the HHS Office of Acquisition at Acquisition_Policy@hhs.gov.

Attachments

Attachment 1 – Class Deviation to HHSAR Part 339, Acquisition of Information Technology; Other Parts; Supply Chain Risk Management

Attachment 1

Class Deviation
to the
Department of Health and Human Services Acquisition Regulation (HHSAR): Part 339, Acquisition of Information Technology; Other Parts; Supply Chain Risk Management

HHSAR Part 339

HHSAR Text Baseline is 48 CFR chapter 3 dated December 19, 2023.
Changes to baseline shown as [**bolded, bracketed additions**] and ~~strikethrough~~ deletions.
HHSAR text unchanged shown as asterisks. And deletions between <less than and greater than> symbols.

PART 339—ACQUISITION OF INFORMATION TECHNOLOGY [(DEVIATION)]

[339.000 Scope of part.]

Subpart 339.1 – General
339.101 Policy.
[339.106 Contract clauses.
339.106-70 Information technology security and privacy clauses.]

Subpart 339.2 – ~~Electronic and Information Technology~~ [Information and Communication Technology]
[339.201 Scope of subpart.]
339.203 Applicability.
339.203-70 [Solicitation provision and contract clauses.] ~~Contract clauses for electronic and Information technology (EIT) acquisitions.~~
339.204 ~~Exceptions.~~
~~339.204-1 Approval of exceptions.~~
339.205 ~~Section 508 accessibility standards for contracts.~~

*****

[339.000 Scope of part. (Deviation)

This part prescribes acquisition policies and procedures for use in acquiring information technology, information and communication technology (ICT), and information technology-related contracts (see 302.101) and applies to both HHS-procured information technology and ICT systems as well as Interagency Acquisitions defined in FAR part 17 and part 317.]

Subpart 339.1 – General [(Deviation)]

339.101 Policy [(Deviation)]

~~In addition to the regulatory guidance in Federal Acquisition Regulation part 39, contracting officers shall collaborate with the requiring activity to ensure information technology (IT) acquisitions for supplies, services, and systems meet the requirements established by the Department of Health and Human Services (HHS).~~

[(a)(1) In acquiring information technology and ICT, including information technology-related contracts which may involve services (including support services), and related resources (see the definition for information technology at FAR 2.101), contracting officers and requiring activities shall include in solicitations and contracts the requirement to comply with the following directives, policies, and procedures in order to protect HHS information, information systems, information technology, and ICT—

(i) The HHS Policy for Information Security and Privacy Protection (IS2P) establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive orders, policies, regulations, standards, and guidance for protecting and controlling HHS sensitive information and ensuring that security requirements are included in acquisitions, solicitations, contracts, purchase orders, and task or delivery orders.

(ii) The HHS policies, security requirements, procedures, and guidance in paragraph (a)(1)(i) of this section apply to all HHS contracts and to contractors, subcontractors, and their employees in the performance of contractual obligations to HHS for information technology products purchased from vendors, as well as for services acquired from contractors and subcontractors or business associates, through contracts and service agreements, in which access to HHS information, HHS sensitive information, (including protected health information (PHI))—

(A) That is created, received, maintained, or transmitted, or that will be stored, generated, accessed, exchanged, processed, or utilized by HHS, an HHS contractor, subcontractor or third-party servicers or associates, or on behalf of any of these entities, in the performance of their contractual obligations to HHS; and

(B) By or on behalf of any of the entities identified in this section, regardless of—

(1) Format; or

(2) Whether it resides on an HHS or a non-HHS system, or with a contractor, subcontractor, or third-party system or electronic information system(s), including cloud services, operating for or on the HHS behalf or as required by contract.

(c) Contractors, subcontractors, and third-party servicers or associates providing support to or on behalf of these entities, shall employ adequate security controls and use appropriate common security configurations available from the National Institute of Standards and Technology (see FAR 39.101(c)) as appropriate in accordance with HHS regulations, policies, and guides, and established service level agreements and individual contracts, business associate agreements, orders, and agreements. Contractors, subcontractors, and third-party servicers and associates will ensure that HHS information or HHS sensitive information that resides on an HHS system or resides on a contractor/subcontractor/third-party entities'/associates' information and communication technology (ICT) system(s), operating for or on HHS behalf, or as required by contract, regardless of form or format, whether electronic or manual, and information systems, are protected from unauthorized access, use, disclosure, modification, or destruction to ensure information security (see FAR 2.101) is provided in order to ensure the integrity, confidentiality, and availability of such information and information systems.]

[339.106 Contract clauses. (Deviation)

339.106-70 Information technology security and privacy clauses. (Deviation)

(a) Contracting officers shall insert the clause at 352.239-71, Security Requirements for Information Technology Resources, in all solicitations, contracts, and orders exceeding the micro-purchase threshold that include information technology services, and the provision 352.239-72, Information Technology Security Plan and Accreditation, in all solicitations exceeding the micro-purchase threshold that include information technology services.

(b) Contracting officers shall insert the clause at 352.239-73, Information System Design and Development, in solicitations, contracts, orders, and agreements where services to perform information system design and development are required.

(c) Contracting officers shall insert the clause at 352.239-74, Information System Hosting, Operation, Maintenance or Use, in solicitations, contracts, orders, and agreements where services to perform information system hosting, operation, maintenance, or use are required.

(d) Contracting officers shall insert the clause at 352.239-75, Security Controls Compliance Testing, in solicitations, contracts, orders, and agreements, when the clauses at 352.239-73, 352.239-74, 352.239-76, and/or 352.239-77 are inserted.

(e) Contracting officers shall insert the clause at 352.239-76, Security Requirements for Government-Owned Contractor-Operated and Contractor-Owned Contractor-Operated Resources, in solicitations, contracts, orders, and agreements involving Government information processed with government-owned contractor-operated and contractor-owned contractor-operated resources.

(f) Contracting officers shall insert the clause at 352.239-77, Cloud Computing Services, in solicitations, contracts, orders, and agreements involving cloud computing services.]

Subpart 339.2 – ~~Electronic and~~ Information [and Communication] Technology [(Deviation)]

[339.201 Scope of subpart. (Deviation)

This subpart applies to the acquisition of Information and Communication Technology (ICT) supplies, products, platforms, information, documentation, and services support. It concerns the access to and use of information and data, by both Federal employees with disabilities, and members of the public with disabilities in accordance with FAR 39.201. This implements HHS policy on Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and the Architectural and Transportation Barriers Compliance Board's (U.S. Access Board) ICT accessibility standards at 36 CFR parts 1193 and 1194 as it applies to contracts and acquisitions when developing, procuring, maintaining, or using ICT.]

339.203 Applicability. [(Deviation)

(a) *General.*

(1) The HHS Policy for Section 508 Compliance and Accessibility of ICT, establishes HHS procedures, responsibilities, and processes for ensuring ICT complies with current Federal law, Executive orders, policies, regulations, standards and guidance for identifying and evaluating HHS ICT and ensuring that Section 508 requirements are included in solicitations, contracts, agreements, purchase orders, and task or delivery orders. Contracting officers shall ensure contractor compliance with the HHS Policy for Section 508 Compliance and Accessibility of ICT.

(2) Solicitations for information technology (*i.e.*, information and communication technology (ICT)) or IT-related supplies, products, platforms, information, and documentation shall require the contractor to submit an HHS Section 508 Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or Accessibility Conformance Report(s) (ACR), based on the Voluntary Product Accessibility Template (see https://www.itic.org/policy/accessibility/vpat). All deliverables resulting from a solicitation must conform to HHS Digital Accessibility standards.]

~~(a) Electronic and information technology (EIT) supplies and services must comply with Section 508 of the Rehabilitation Act (the Act) of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, and the Architectural and Transportation Barriers Compliance Board (Access Board) Electronic and Information Accessibility Standards (36 CFR part 1194). Requiring activities must consult with their Section 508 Official or designee to determine if the contractor should be responsible for compliance with EIT accessibility standards which apply to Web site content and communications material.~~

~~(1) When conducting a procurement and employing the best value continuum, the solicitation shall include a separate technical evaluation factor developed by the contracting officer, requiring activity, and the Operating Division (OPDIV) Section 508 Official or designee.~~

~~(2) At a minimum, solicitations for supplies and services shall require the submission of a Section 508 Product Assessment Template (See *http://www.hhs.gov/web/508* for the template). Solicitations for services shall include any other pertinent information that the contracting officer deems necessary to evaluate the offeror's ability to meet the applicable Section 508 accessibility standards.~~

~~(3) The HHS Operating Division or Staff Division (OPDIV or STAFFDIV) Section 508 Official or designee is responsible for providing technical assistance in development of Section 508 evaluation factors.~~

~~(4) Before conducting negotiations or making an award, the contracting officer shall provide a summary of the Source Selection Evaluation Team's (SSET) assessment of offeror responses to the solicitation's Section 508 evaluation factor. This summary shall be submitted for review by the Section 508 Official or designee. The Section 508 Official or designee shall indicate approval or disapproval of the SSET assessment. The contracting officer shall coordinate the resolution of any issues raised by the Section 508 Official or designee with the chair of the SSET or requiring activity representative, as appropriate. The acquisition process shall not proceed until the Section 508 Official or designee approves the SSET assessment. The contracting officer shall include the assessment in the official contract file. See 339.204-1 regarding processing exception determination requests.~~

~~(b) When acquiring commercial items, if no commercially available supplies or services meet all of the applicable Section 508 accessibility standards, OPDIVs or STAFFDIVs shall, under the direction and approval of the Section 508 Official or designee, acquire the supplies and services that best meet the applicable Section 508 accessibility standards. Process exception determinations for EIT supplies and services not meeting applicable Section 508 accessibility standards in accordance with 339.204-1.~~

339.203-70 [Solicitation provision and contract clauses] ~~Contract clauses for electronic and Information technology (EIT) acquisitions~~. [(Deviation)]

(a) The contracting officer shall insert the provision at 352.239-~~73~~**[78]**, ~~Electronic and~~ Information **[and Communication]**Technology Accessibility Notice, in all solicitations.

(b) The contracting officer shall insert the clause at 352.239-~~74~~**[79]**, ~~Electronic and~~ Information **[and Communication]** Technology Accessibility, in all **[solicitations and]** contracts~~ and orders~~.

339.204 ~~Exceptions.~~[(Deviation)]

339.204-1 Approval of exceptions.[(Deviation)]

(a) Procedures to document exception and determination requests are set by the OPDIV Section 508 Official.

(b) In the development of an acquisition plan (AP) or other acquisition request document, the contracting officer shall ensure that all Section 508 exception determination requests for applicable EIT requirements are:

(1) Documented and certified in accordance with the requirements of the HHS Section 508 policy;

(2) Signed by the requestor in the requiring activity;

(3) Certified and approved by the OPDIV Section 508 Official or designee; and

(4) Included in the AP or other acquisition request document provided by the requiring activity to the contracting office.

(c) For instances with an existing technical evaluation and no organization's proposed supplies or services meet all of the Section 508 accessibility standards; in order to proceed with the acquisition, the requiring activity shall provide an exception determination request along with the technical evaluation team's assessment of the Section 508 evaluation factor to the designated Section 508 Official or designee for review and approval or disapproval. The contracting officer shall include the Section 508 Official's or designee's approval or disapproval of the exception determination request in the official contract file and reference it, as appropriate, in all source selection documents. For further information, see HHS Section 508 Policy on *http://www.hhs.gov/web/508*.

339.205 Section 508 accessibility standards for contracts. [(Deviation)]

(a) Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794(d)), as amended by the Workforce Investment Act of 1998 (Section 508), specifies the applicable accessibility standards for all new solicitations and new or existing contracts or orders, regardless of EIT dollar amount.

(b) The requiring activity shall consult with the OPDIV or STAFFDIV Section 508 Official or designee, as necessary, to determine the applicability of Section 508, identify applicable Section 508 accessibility standards, and resolve any related issues before forwarding a request to the contracting or procurement office for the acquisition of EIT supplies and services including Web site content and communications material for which the contractor must meet EIT accessibility standards.

(c) Based on those discussions, the requiring activity shall provide a statement in the AP (or other acquisition request document) for Section 508 applicability. See 307.105. If Section 508 applies to an acquisition, include the provision at 352.239-73, Electronic and Information Technology and Accessibility Notice, language in a separate, clearly designated, section of the statement of work or performance work statement, along with any additional information applicable to the acquisition's Section 508 accessibility standards (e.g., the list of applicable accessibility standards of the Access Board EIT Accessibility Standards (36 CFR part 1194)). If an AP does not address Section 508 applicability and it appears an acquisition involves Section 508, or if the discussion of Section 508 applicability to the acquisition is inadequate or incomplete, the contracting officer shall request the requiring activity modify the AP accordingly.

(d) Items provided incidental to contract administration are not subject to this section.

(e) The OPDIV Section 508 Official or designee may, at his or her discretion, require review and approval of solicitations and contracts for EIT supplies and services.

Class Deviation Affected Parts to HHSAR Part 339

PART 302 – DEFINITIONS OF WORDS AND TERMS [(DEVIATION)]

[302.000 Scope of part.]

Subpart 302.1 - Definitions
302.101 Definitions.

[302.000 Scope of part. (Deviation)

(a) This part -

(1) Defines words and terms that are frequently used in the HHSAR;

(2) Provides cross-references to other definitions in the HHSAR of the same word or term; and

(3) Provides for the incorporation of these definitions in solicitations and contracts by reference.

(b) Other parts, subparts, and sections of this regulation (48 CFR chapter 3) may define other words or terms and those definitions only apply to the part, subpart, or section where the word or term is defined.]

Subpart 302.1 – Definitions [(Deviation)]

302.101 Definitions. [(Deviation)]

[(a) A word or a term, defined in this section, has the same meaning throughout this regulation (48 CFR chapter 3), unless -

(1) The context in which the word or term is used clearly requires a different meaning; or

(2) Another HHSAR part, subpart, or section provides a different definition for the particular part or portion of the part.

(b) If a word or term that is defined in this section is defined differently in another part, subpart, or section of this regulation (48 CFR chapter 3), the definition in -

(1) This section includes a cross-reference to the other definitions; and

(2) That part, subpart, or section applies to the word or term when used in that part, subpart, or section.]

~~(a)~~ **[*Agency head or head of the agency*]**, unless otherwise stated, means the Secretary of Health and Human Services or specified designee. **[When delegated by the Secretary, the specific designee will be reflected in the specific part, subpart, or section where a specified designee other than the Secretary has been designated.]**

[*Business associate (*see 45 CFR 160.103), except as provided in paragraph (2) of this definition, means with respect to a covered entity, a person who –

~~(1)~~ On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by contracts or agreements issued pursuant to the HHSAR, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

~~(2)~~ Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

~~(3)~~ A covered entity may be a business associate of another covered entity.

~~(4)~~ For use in part 324, see the definition at 324.101.]

[*Business associate agreement* means the agreement, or other arrangement, as dictated by the HIPAA Privacy Rule (45 CFR 160), between an HHS covered entity and a business associate, which must be entered into in addition to the underlying contract for services and before any disclosure (see 45 CFR 160.103) of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of an HHS entity.]

~~(b) *Contracting Officer's Representative (COR)* is a Federal employee designated in writing by a contracting officer to act as the contracting officer's representative in monitoring and administering specified aspects of contractor performance after award of a contract or order. In accordance with local procedures, operating divisions (OPDIVs) or staff divisions (STAFFDIVs) may designate CORs for firm fixed-price contracts or orders. COR's responsibilities may include verifying that:~~

~~(1) The contractor's performance meets the standards set forth in the contract or order;~~

~~(2) The contractor meets the contract or order's technical requirements by the specified delivery date(s) or within the period of performance; and~~

~~(3) The contractor performs within cost ceiling stated in the contract or order. CORs must meet the training and certification requirements specified in PGI Part 301.604.~~

[*Covered entity* (see 45 CFR 160.103) means—

(1) A health plan (see 45 CFR 160.103);

(2) A health care clearinghouse (see 45 CFR 160.103); or

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this chapter (see 45 CFR 160.103).]

(c) [***Head of the contracting activity (HCA)***] ~~is~~ **[means]** an official having overall responsibility for managing a contracting activity, *i.e.*, the organization within an **[Operating Division (]**OPDIV**[)]** or **[Staff Division (]**STAFFDIV**[)]** or other HHS organization which has been delegated broad authority regarding the conduct of acquisition functions.

[*HHS Information Security Rules of Behavior for Organizational Users* means the "HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy" which is a set of HHS rules that describes the responsibilities and expected behavior of users of HHS information or information systems.]

[*HHS sensitive information* means all HHS data, on any storage media or in any form or format, which requires confidentiality, integrity, and availability protection due to the risk of harm that could result to interests of HHS, other agencies or entities, or individuals from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes –

(1) Information where the improper use or disclosure of which could adversely affect the ability of HHS to accomplish its mission, *i.e.*, HHS proprietary information;

(2) Records about individuals requiring protection under laws and regulations such as the E-Government Act, Privacy Act, and the HIPAA Privacy Rule, or based on a data use agreement or a promise or assurance of confidentiality; and

(3) Information that would be exempt from disclosure if requested under the Freedom of Information Act.

(4) Examples of HHS sensitive information include–

(i) Individually-identifiable medical, benefits, and personnel information;

(ii) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, security-sensitive, procurement-sensitive, investigatory, and law enforcement information;

(iii) Controlled unclassified information;

(iv) Information that would be confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and

(v) Other information which, if released, could result in a violation of law or agreement, could cause harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.]

[*HIPAA Rules* mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR part 160 and part 164.]

[*Information* means 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 (see OMB Circular A-130).]

[*Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.]

[*Information and communication technology (ICT) also means* information technology (see FAR 2.101 for definitions).]

[*Organized health care arrangement* (see 45 CFR 160.103) means:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.]

[*Information technology-related contracts* means those contracts that include services (including support services), and related resources for information technology.]

[*Privacy officer* means the HHS official with responsibility for implementing and oversight of privacy related policies and practices that impact a given HHS acquisition. Depending on the specific acquisition privacy requirement, the privacy officer may be the Senior Agency Official for Privacy (Agency level); the Senior Official for Privacy (OPDIV level); or the privacy officer responsible for the appropriate operational privacy posture for a system or program (requirement level).]

***[Protected health information (PHI)* (see 45 CFR 160.103) means information subject to the HIPAA Privacy Rule, *i.e.*, individually identifiable health information:**

(1) Except as provided in paragraph (2) of this definition, that is –

(i) Transmitted by electronic media;

(ii) Maintained in electronic media; or

(iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

(i) In education records covered by the Family Educational Rights and Privacy Act (20 U.S.C. 1232g);

(ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

(iii) In employment records held by a covered entity in its role as employer; and

(iv) Regarding a person who has been deceased for more than 50 years.]

[*Security plan* means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.]

PART 304 – ADMINISTRATIVE MATTERS [(DEVIATION)]

****

Subpart 304.13—Personal Identity Verification
~~304.1300 Policy.~~
[304.1301 Policy.
304.1303 Contract clause.]

****

[Subpart 304.19—Basic Safeguarding of Covered Contractor Information Systems
304.1900-70 Scope of subpart.
304.1901 Definitions.
304.1902 Applicability.
304.1903 Contract clause.
304.1970 Information security policy—contractor general responsibilities.]

Subpart 304.70[—Records Management] ~~[Reserved]~~
[304.7000 Scope of subpart.
304.7001 Applicability.
304.7002 Definition.
304.7003 Policy.
304.7004 Contract clause.]

*****

Subpart 304.13—Personal Identity Verification [(Deviation)]

~~304.1300 Policy~~ [(Deviation)]

~~To ensure compliance with Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD-12) and the Presidential Cross Agency Priority for strong authentication, contracting officers shall provide in each acquisition those HSPD-12 requirements necessary for contract performance.~~

[304.1301 Policy. (Deviation)

(a) HHS follows National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication (PUB) Number 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, and OMB implementation guidance for personal identity verification, for all affected contractor and subcontractor personnel when contract performance requires contractors to have routine physical access to a federally-controlled facility and/or routine physical and logical access to a federally-controlled information system.

(c) Operating Divisions and Staff Divisions must designate an official responsible for verifying contractor employees' personal identity.

304.1303 Contract clause. (Deviation)

The contracting officer shall insert the clause at 352.204-73, Contractor Personnel Security and Agency Access, in solicitations and contracts (including task orders, if appropriate), exceeding the micro-purchase threshold, when contract performance requires contractors to have routine physical access to a federally-controlled facility and/or routine physical and/or logical access to a Departmental/federally-controlled information system.]

****

[Subpart 304.19—Basic Safeguarding of Covered Contractor Information Systems (Deviation)

304.1900-70 Scope of subpart. (Deviation)

This subpart prescribes policies and procedures for information security and protection of HHS information, information systems, and sensitive information, including controlled unclassified information.

304.1901 Definitions. (Deviation)

As used in this subpart –

***Breach* means 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 personally identifiable information for an other than authorized purpose.

***Controlled unclassified information (CUI)* means information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.**

***Incident* means an occurrence that—**

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies.

304.1902 Applicability. (Deviation)

This subpart applies to all HHS acquisitions, including acquisitions of commercial products and commercial services other than commercially available off-the-shelf items, when a contractor's information system or information system(s) accessed, may contain HHS information.

304.1903 Contract clause. (Deviation)

The contracting officer shall insert clause 352.204-71, Information and Information Systems Security, when—

(a) The clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903; or

(b) In solicitations and contracts requiring information security and/or physical access security.

304.1970 Information security policy—contractor general responsibilities. (Deviation)

Contractors, subcontractors, business associates and their employees who are users of HHS information or information systems, or have access to HHS information and HHS sensitive information shall—

(a) Comply with all HHS information security and privacy program policies, procedures, practices and related contract requirements, specifications, and clauses. This includes complying with HHS privacy and confidentiality laws and HHS implementing regulations, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191)(45 CFR sec. 160 and 164), the Privacy Act of 1974(5 U.S.C. 522a), the E-Government Act of 2002, NIST SP 800-53, and Executive Order 13556, Controlled Unclassified Information (implemented at 32 CFR, part 2002);

(b) Complete HHS security awareness training on an annual basis;

(c) Complete HHS Privacy and HIPAA Training on an annual basis. All users are required to complete annual privacy training, regardless of access to protected health information (PHI);

(d) Use information provided by HHS or collected by the contractor or its employees, subcontractors, or business associates on behalf of HHS only for the purpose of carrying out the provisions of the contract. The information must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors is under the supervision of the contractor. Each contractor employee or

subcontractors at any tier to whom any HHS records may be made available or disclosed must be notified in writing by the contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein. The confidentiality, integrity, and availability of such information must be protected in accordance with HHS policies. Unauthorized disclosure of information will be subject to the HHS sanction policies and/or governed by the following laws and regulations:

(i) 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);

(ii) 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and

(iii) 44 U.S.C. chapter 35, subchapter I (Paperwork Reduction Act).

(e) Submit a completed non-disclosure agreement, provided by the contracting officer or contracting officer's representative (COR), for each employee, or subcontractor business associate having access to non-public government information under an HHS contract. The non-disclosure agreements shall be submitted to the contracting officer prior to the performance of work;

(f) Comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; OMB M-19-17; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, part 1, section 1.2;

(g) Report all actual or suspected incidents and breaches and report the information to the contracting officer and COR, as identified in the contract or as directed in the contract, within one hour of discovery or suspicion;

(h) Comply with HHS policy as it relates to personnel security and suitability program requirements for background screening of both employees and non-employees who have access to HHS information systems and data;

(i) Submit a roster containing the name, position, e-mail address, phone number, and responsibilities of each employee, including subcontractors or business associates, performing work under a contract to develop, access, host, or maintain a government information system(s). The roster must be submitted to the contracting officer within the stated number of days from the effective date of the contract, as provided by the contracting officer. Revisions to the roster as a result of staffing changes must be submitted within the number of days of the change provided by the contracting officer. The contracting officer, or the COR, will notify the contractor of the appropriate level of investigation required for each staff member based on the information provided on the roster. If an employee is filling a new position, the contractor must provide a position description and the Government will determine the appropriate suitability level;

(j) Comply with directions that may be issued by the contracting officer or COR, or from an incident response or other designated representative through the contracting officer or COR, directing specific activities when an incident or breach occurs;

(k) Require contractor employees, subcontractors, or business associates to sign an acknowledgment that they have read, understand, and agree to abide by the *HHS Information Technology General Rules of Behavior, HHS Rules of Behavior for Privileged Users*, and any other rules of behavior provided by the contracting officer, as applicable as required by FAR 39.105, Privacy, and clause 352.204-71, Information and Information Systems Security, on an annual basis. The Rules of Behavior describe the responsibilities and expected behavior of contractors, subcontractors, business associates and their employees who are users of HHS information or information systems, information assets and resources, or have access to HHS information;

(l) Maintain records and compliance reports regarding the HIPAA Rules (see 302.101) in order to provide such information to HHS upon request to ascertain whether the business associate is complying with all applicable provisions under the rules' regulatory requirements. Document and report the accidental disposal or destruction of a record, when done without proper authorization in accordance with HHS policies; and

(m) Flow down these requirements in all subcontracts and business associate agreements (see 324.103-70(e)), at any tier, as provided in the clause at 352.204-71, Information and Information Systems Security.

304.1903 Contract clause. (Deviation)

The contracting officer shall insert clause 352.204-71, Information and Information Systems Security, when—

(a) The clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems is required to be included in accordance with FAR 4.1903; or

(b) In solicitations and contracts requiring information security and/or physical access security.]

****

Subpart 304.70[—Records Management (Deviation)] ~~[Reserved]~~

304.7000 Scope of subpart. (Deviation)

This subpart implements National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. 21, 29, 31, and 33), NARA regulations at 36 CFR chapter XII subchapter B, and those policies associated with the safeguarding of Federal records covered by the Privacy Act of 1974 (5 U.S.C. 552a).

304.7001 Applicability. (Deviation)

This subpart applies to contracts that include Federal records, as defined at 304.7002.

304.7002 Definition. (Deviation)

As used in this subpart—

Federal record **means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. See 44 U.S.C. 3301.**

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with deliverables.

(2) ***Recorded information*** **means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)**

(3) ***Personal materials*** **means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)**

304.7003 Policy. (Deviation)

(a) Program/project managers, HHS records officers, and the contracting officer shall ensure that applicable contracts contain records management obligations.

(b) The contracting officer shall promptly report to the OPDIV/STAFFDIV Records Officer when notified by the contractor of any willful and unlawful destruction, damage or alienation of Federal records which is subject to the fines and penalties imposed by 18 U.S.C. 2701. See 36 CFR 1230.

(c) Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the contracting officer.

(d) The contractor shall not remove Federal records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the contracting officer.

(e) Upon award, the contracting officer shall ensure that the OPDIV/STAFFDIV Records Officer provides information regarding required records management training to the contractor.

304.7004 Contract clause. (Deviation)

The contracting officer shall insert the clause at 352.204-72, Records Management, in solicitations and contracts that include Federal records, as defined at 304.7002.]

*****

PART 324 – PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION [(DEVIATION)]

*****

Subpart 324.1 - Protection of Individual Privacy [(Deviation)]

[324.101 Definitions. (Deviation)

As used in this subpart –

Business associate (*see 45 CFR 160.103)*:

(1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who –

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in this part) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by contracts or agreements issued pursuant to the HHSAR, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity may be a business associate of another covered entity.

(3) *Business associate* includes the following:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

***Covered entity (*see 45 CFR 160.103) means the definition provided at 302.101.**

***Healthcare component* means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 CFR 164.105(a)(2)(iii)(D) (see 45 CFR 164.103).**

***HIPAA Rules* means the definition provided at 302.101.**

***Hybrid entity* means a single legal entity –**

(1) That is a covered entity;

(2) Whose business activities include both covered and non-covered functions; and

(3) That designates health care components in accordance with 45 CFR 164.105(a)(2)(iii)(D).

Organized health care arrangement **(see 45 CFR 160.103) means:**

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.]

[324.102 General. (Deviation)

HHS rules implementing the Privacy Act of 1974 are in 45 CFR 5b, Privacy Act Regulations.]

~~324.103 Procedures for the Privacy Act.~~[(Deviation)]

~~(a) The contracting officer shall review all acquisition request documentation to determine whether the requirements of the Privacy Act of 1974 (5 U.S.C. 552a) are applicable. The Privacy Act requirements apply when a contract or order requires the contractor to design, develop, or operate any Privacy Act system of records on individuals to accomplish an agency function. When applicable, the contracting officer shall include the two Privacy Act clauses required by Federal Acquisition Regulation (FAR) 24.104 in the solicitation and contract or order. In addition, the contracting officer shall include the two FAR Privacy Act clauses, and other pertinent information specified in this subpart, in any modification which results in the Privacy Act requirements becoming applicable to a contract or order.~~

~~(b) The contracting officer shall ensure that the statement of work or performance work statement (SOW or PWS) specifies the system(s) of records or proposed system(s) of records to which the Privacy Act and the implementing regulations are applicable or may be applicable. The contracting officer shall send the contractor a copy of 45 CFR part 5b, which includes the rules of conduct and other Privacy Act requirements.~~

~~(c) The contracting officer shall ensure that the contract SOW or PWS specifies for both the Privacy Act and the Federal Records Act the disposition to be made of the system(s) of records upon completion of contract performance. The contract SOW or PWS may require the contractor to destroy the records, remove personal identifiers, or turn the records over to the contracting officer. If there is a legitimate need for a contractor to keep copies of the records after completion of a contract, the contractor must take measures, as approved by the contracting officer, to keep the records confidential and protect the individuals' privacy.~~

~~(d) For any acquisition subject to Privacy Act requirements, the requiring activity shall prepare and have published in the Federal Register a "system notice," describing the Department of Health and Human Services' (HHS) intent to establish a new system of records on individuals, to make modifications to an existing system, or to disclose information in regard to an existing system. The requiring activity shall attach a copy of the system notice to the acquisition plan or other acquisition request documentation. If a system notice is not attached, the contracting officer shall inquire about its status and shall obtain a copy from the requiring activity for inclusion in the contract file. If a notice for the system of records has not been published in the Federal Register, the contracting officer may proceed with the acquisition but shall not award the contract until the system notice is published and the contracting officer verifies its publication.~~

[324.103-70 Protection of privacy—general requirements and procedures related to business associate agreements. (Deviation)

(a) To ensure compliance with unique responsibilities to protected health information, contractors performing under HHS contracts subject to protected health information (PHI) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191) shall comply with the HIPAA Rules, the requirements of this part, and the clause prescribed at 304.1903, 352.204-71, Information and Information Systems Security.

(b) The Secretary has designated HHS as a covered entity (further designated as a "hybrid entity"), see 45 CFR 164.103 and 164.105(a)), and has designated four HHS divisions as healthcare components under HIPAA, including —

(1) The Centers for Medicare and Medicaid Services (CMS), insofar as it operates the fee-for-service Medicare program;

(2) The Program Support Center (PSC), Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers;

(3) The World Trade Center (WTC) Health Program; and

(4) The Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions.

(c) *HIPAA business associate agreements*. Under the HIPAA Privacy and Security Rules (see 45 CFR 164), pursuant to 45 CFR 164.502(e)(1), a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor of a covered entity's business associate. Additionally, a business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with 45 CFR 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. The satisfactory assurances required by 45 CFR 164.504(e)(1) shall be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of 45 CFR 164.504(e). The contracts shall also include breach reporting policies and procedures for suspected or confirmed breaches of protected health information. The contract shall impose a duty to cooperate with the healthcare component and/or HHS breach investigation and response and must require all subcontractors to comply with the same HIPAA Rules requirements as a condition of receiving government data.

(d) *Healthcare components required to execute a business associate agreement or other written agreement or arrangement, become HHS business associates.* Business associate

agreements may be issued by other HHS programs in support of HHS. The HIPAA Privacy Rule requires HHS to execute compliant business associate agreements with persons or entities that create, receive, maintain, or transmit PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of HHS.

(1) Healthcare components awarding contracts, agreements, or other arrangements that include purchase/delivery orders, call orders, modifications, and governmentwide purchase card transactions to help in the delivery of these services to HHS, shall obtain a satisfactory assurance from these contractors by executing business associate agreements.

(2) Contractors or other entities supporting HHS required to create, receive, maintain, or transmit PHI shall be required to execute a business associate agreement as mandated by the HIPAA Privacy Rule and requested by the contracting officer, the contracting officer's representative, or the cognizant privacy officer—

(i) Whether via a contract or agreement with HHS; or

(ii) Whether provided from or through any HHS Operating or Staff Division contract for supplies, services or support that involves performing a certain activity, function, or service to, for, or on behalf of HHS.

(e) ***Business associate agreement flow down to subcontractors*****. A prime contractor required to execute a business associate agreement shall also obtain a satisfactory assurance, in the form of a business associate agreement, of its subcontractors who will also create, receive, maintain, or transmit PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA Rules requirements to the same degree as the contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits PHI or that will store, generate, access, exchange, process, or utilize such PHI under a contract or agreement is required to execute a business associate agreement with each of its subcontractors which also obligates the subcontractor (*i.e.*, also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to PHI that is required of the covered entity and the prime contractor.**

~~**324.104 Restrictions on Contractor Access to Government or Third Party Information.**~~**[(Deviation)]**

~~The contracting officer shall establish the restrictions that govern the contractor employees' access to Government or third party information in order to protect the information from unauthorized use or disclosure.~~

324.10[4]~~5~~ Contract clauses. [(Deviation)]

~~(a) The contracting officer shall insert the clause at 352.224-70, Privacy Act, in solicitations, contracts, and orders that require the design, development, or operation of a system~~

~~of records. to notify the contractor that it and its employees are subject to criminal penalties for violations of the Privacy Act (5 U.S.C. 552a(i)) to the same extent as HHS employees. The clause also requires the contractor to ensure each of its employees knows the prescribed rules of conduct in 45 CFR part 5b and each contractor employee is aware that he or she is subject to criminal penalties for violations of the Privacy Act. These requirements also apply to all subcontracts awarded under the contract or order that require the design, development, or operation of a system of records.~~

[(a) The contracting officer shall insert the clause at 352.224-70, Notification of System of Records Notice(s), in solicitations, contracts, and orders that require the design, development, or operation of a system of records, as defined in the Privacy Act of 1974 (5 U.S.C. 552a). "System of records" is defined in the Privacy Act as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." The contracting officer shall insert into the clause the System of Records Notice(s) applicable to the resulting contract or order.]

~~(b)~~ The contracting officer shall insert the clause at 352.224-71, Confidential Information, in solicitations, contracts, and orders that require access to Government or to third party **[Confidential I]**~~i~~nformation.

[Subpart 324.2 – Freedom of Information Act (Deviation)

324.203 Policy. (Deviation)

(a) The HHS regulation implementing the Freedom of Information Act (FOIA), 5 U.S.C. 552, is set forth in 45 CFR part 5. Each OPDIV shall follow its internal guidance for the processing of FOIA requests.

(b) The contracting officer, upon receiving a FOIA request, shall follow HHS and OPDIV procedures. Further information can be located at https://www.hhs.gov/foia/index.html.]

*****

PART 352—SOLICITATION PROVISIONS AND CONTRACT CLAUSES [(DEVIATION)]

Subpart 352.2—Text of Provisions and Clauses [(Deviation)]

*****

[352.204-73 Contractor Personnel Security and Agency Access. (Deviation)

As prescribed in 304.1303, insert the following clause:

CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS (FEB 2024) (DEVIATION)

(a) ***Definitions.*** **As used in this clause—**

Agency access **means access to HHS facilities, sensitive information, information systems or other HHS resources.**

Applicant **means a contractor employee for whom the Contractor applies for an HHS identification card.**

Contractor employee **means a prime contractor and subcontractor employee who requires agency access to perform work under an HHS contract.**

Identification card (or "ID card") **means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by HHS, or a non-PIV card issued by another Federal agency and approved by HHS. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.**

Issuing office **means the HHS entity that issues identification cards to contractor employees.**

Local security servicing organization **means the HHS entity that provides security services to the HHS organization sponsoring the contract.**

(b) ***Risk and sensitivity level designations*****. For contracts requiring access to HHS facilities, sensitive information, information systems or other HHS resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. HHS will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. The position sensitivity designation levels that apply will be identified in the contract. The following risk and sensitivity level**

designations and associated level of processing are required, and each level includes the prior levels—

(1) Low risk level: National Agency Check with Written Inquiries (NACI);

(2) Moderate risk level: Minimum Background Investigation (MBI); and

(3) High risk level: Background Investigation.

(c) *Security clearances.* Contractor employees may also be required to obtain security clearances (*i.e.*, Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in HHS will be processed according to the HHS Personnel Security and Suitability Program, HHS Instruction 731-1, and the Department of Defense National Industrial Security Program Operating Manual (NISPOM).

(d) *Pre-screening of contractor employees*. The Contractor must pre-screen individuals designated for employment under any HHS contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to HHS for agency access. HHS may decline to grant agency access to a contractor employee for reasons including, but not limited to—

(1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;

(2) Falsification of information entered on forms or of other documents submitted;

(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and

(4) Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

(e) *Citizenship status*. The Contractor must monitor a non-citizen's continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

(f) ***Background investigation and adjudication*****. A contractor employee must have a favorable adjudication of background investigation before HHS will issue an ID card to the contractor employee granting access to HHS facilities, sensitive information, information systems or other HHS resources. HHS may accept favorable adjudications of background investigations from other Federal agencies when applicants have held PIV cards issued by those agencies with no break in service. HHS may also accept PIV-I (Interoperable) cards issued by an authorized PIV-1 issuer as evidence of identity. A favorable adjudication does not preclude HHS from initiating a new investigation when deemed necessary. At a minimum, the FBI National Criminal History Check (fingerprint check) must be favorably completed before an HHS identification card can be issued. Each Contractor must use the Office of Personnel Management's (OPM) e-QIP system, or successor system identified by HHS, to complete any required investigative forms. Instructions for obtaining fingerprints will be provided by the COR or Contracting Officer. The HHS Assistant Secretary for Administration, Program Support Center (PSC), or authorized HHS designee, is responsible for adjudicating the suitability of contractor employees.**

(g) ***Agency access denied*****. Upon contract award, HHS will initiate the agency access procedure for all contractor employees requiring access to HHS facilities, sensitive information, controlled unclassified information, information systems, and other HHS resources for contract performance. HHS may deny agency access to any individual about whom an adverse suitability determination is made. Failure to submit the required security information or to truthfully answer all questions shall constitute grounds for denial of access. The Contractor must not provide agency access to contractor employees until the COR or Contracting Officer provides notice of approval, which is authorized only by the PSC, or authorized HHS designee. Where a proposed contractor employee is denied agency access by the Government or, if for any reason a proposed application is withdrawn by the Contractor during the agency access process, the additional costs and administrative burden for conducting additional background investigations caused by a lack of effective pre-screening or planning on the part of the Contractor may be considered as part of the Contractor's overall performance evaluation.**

(h) ***Identification card application process*****. The COR will be the HHS ID card Sponsor and point of contact for the Contractor's application for an HHS ID card. The COR shall review and approve the HHS ID card application before an ID card is issued to the applicant. An applicant may be issued either a Personal Identity Verification (PIV) card that meets the standards of Homeland Presidential Security Directive (HSPD-12), or an applicant may be issued a non-PIV card. Generally, a non-PIV card will be issued for contracts that expire in six months or less, including option periods. The COR may request the issuing office to waive the six-month eligibility requirement when it is in HHS interest for contract performance. The following applies—**

(1) PIV card. The applicant must complete an HHS on-line application for a PIV card;

(2) Non-PIV card. The applicant must complete and submit a hard copy of the necessary form(s) to be provided to Contractor by COR/Sponsor) to the COR/Sponsor; and

(3) Regardless of the type of card to be issued (PIV or non-PIV), the applicant must appear in person to provide two forms of identity source documents in original form to HHS. The identity source documents must come from the list of acceptable documents included in Form F-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid State or Federal government-issued picture identification. For a PIV card, the applicant may be required to appear in-person a second time for enrollment and activation.

(i) ***Identification card custody and control*****. The Contractor is responsible for the custody and control of all forms of government identification issued by HHS to contractor employees for access to HHS facilities, sensitive information, information systems and other HHS resources. The Contractor shall:**

(1) Provide a listing of personnel for whom an identification (ID) card is requested to the COR who will provide a copy of the listing to the card issuing office. This may include Contractor and subcontractor personnel. Follow issuing office directions for submittal of an application package(s).

(2) While visiting or performing work on an HHS facility, as specified by the issuing office or COR, ensure that contractor employees prominently display their ID card.

(3) Immediately notify the COR or, if the COR is unavailable, the Contracting Officer when a contractor employee's status changes and no longer requires agency access (*e.g.*, employee's transfer, completion of a project, retirement, removal from work on the contract, or termination of employment) that may affect the employee's eligibility for access to the facility, sensitive information, or resources.

(4) Promptly deliver to the issuing office: (a) all ID cards assigned to an employee who no longer requires access to the facility; and (b) all expired ID cards within five (5) days of their expiration or all cards at time of contract termination, whichever occurs first.

(5) Immediately report any lost or stolen ID cards to the issuing office and follow its instructions.

(i) The Contractor is responsible for maintaining and safeguarding the HHS ID card upon issuance to the contractor employee. The Contractor must ensure that contractor employees comply with HHS requirements concerning the renewal, loss, theft, or damage of an ID card. The Contractor must immediately notify the COR or, if the COR is unavailable, the Contracting Officer when an ID card is lost, stolen or damaged.

(ii) Failure to comply with the requirements for custody and control of HHS ID cards may result in withholding final payment or contract termination based on the

potential for serious harm caused by inappropriate access to HHS facilities, sensitive information, information systems or other HHS resources.

(iii) Specific actions and activities are required in certain events—

(A) *Renewal.* A contractor employee's HHS issued ID card is valid for a maximum of three years or until the contract expiration date (including option periods), whichever occurs first. The renewal process should begin six weeks before the PIV card expiration date. If a PIV card is not renewed before it expires, the contractor employee will be required to sign-in daily for facility access and may have limited access to information systems and other resources.

(B) *Lost/stolen*. Immediately upon detection, the Contractor or contractor employee must report a lost or stolen HHS ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local servicing security organization. The Contractor must submit an incident report within 48 hours, through the COR or, if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization describing the circumstances of the loss or theft. The Contractor must also report a lost or stolen PIV card through the HHS on-line registration system. If the loss or theft is reported by the Contractor to the local police, a copy of the police report must be provided to the COR or Contracting Officer. From the date of notification to HHS, the Contractor must wait three days before getting a replacement ID card. During the 3-day wait period, the contractor employee must sign in daily for facility access.

(C) *Replacement.* An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a continuing need for agency access to perform work under the contract.

(D) *Surrender of ID cards*. Upon notification that routine access to HHS facilities, sensitive information, information systems or other HHS resources is no longer required, the Contractor must surrender the HHS issued ID card to the COR, or if the COR is unavailable, the Contracting Officer, the issuing office, or the local security servicing organization in accordance with agency procedures.

(j) *Flow down of clause*. The Contractor is required to include this clause in any subcontracts at any tier that require the subcontractor or subcontractor's employees to have access to HHS facilities, sensitive information, information systems or other resources.

(End of clause)]

[352.204-71 Information and Information Systems Security. (Deviation)

As prescribed in 304.1903, insert the following clause:

INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2024) (DEVIATION)

(a) *Definitions*. As used in this clause—

Breach **means 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 personally identifiable information for an other than authorized purpose.

Business associate (**see 45 CFR 160.103), except as provided in paragraph (2) of this definition, business associate means, with respect to a covered entity, a person who -**

(1) On behalf of such covered entity or of an organized health care arrangement (as defined in this clause) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this contract or agreement, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or

(2) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR section 164.501), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(3) A covered entity may be a business associate of another covered entity.

(4) *Business associate* includes the following:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(5) *Business associate* does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.

***Business associate agreement* means the agreement, or other arrangement, as dictated by the HIPAA Privacy Rule (45 CFR 160), between an HHS covered entity and a business associate, which must be entered into in addition to the underlying contract for services and before any disclosure (see 45 CFR 160.103) of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of an HHS entity.**

***Controlled unclassified information (CUI)* means information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.**

***Healthcare component* means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 CFR 164.105(a)(2)(iii)(D) (see 45 CFR 164.103). The Secretary of HHS has designated HHS as a covered entity (further designated as a "hybrid entity"), and has also designated four HHS divisions as healthcare components under HIPAA, including —**

(1) The Centers for Medicare and Medicaid Services (CMS), insofar as it operates the fee-for-service Medicare program;

(2) The Program Support Center (PSC), Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers;

(3) The World Trade Center (WTC) Health Program; and,

(4) The Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions.

HHS Information Technology General Rules of Behavior **means a set of HHS rules that describes the responsibilities and expected behavior of users of HHS information or information systems.**

HHS sensitive information **means all HHS data, on any storage media or in any form or format, which requires confidentiality, integrity, and availability protection due to the risk of harm that could result to interests of HHS, other agencies or entities, or individuals from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes—**

(1) Information where the improper use or disclosure could adversely affect the ability of HHS to accomplish its mission, *i.e.*, HHS proprietary information;

(2) Records about individuals requiring protection under laws and regulations such as the E-Government Act, Privacy Act and the HIPAA Privacy Rule, or based on a data use agreement or a promise or assurance of confidentiality; and

(3) Information that would be exempt from disclosure if requested under the Freedom of Information Act. Examples of HHS sensitive information include—

(i) Individually-identifiable medical, benefits, and personnel information;

(ii) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, security-sensitive, procurement-sensitive, investigatory, and law enforcement information;

(iii) Controlled unclassified information;

(iv) Information that would be confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and

(v) Other information which, if released, could result in a violation of law or agreement, could cause harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

HIPAA Rules **means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and part 164.**

Incident **means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies.**

Information system **means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.**

Information system security plan **means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.**

Information technology **(see FAR 2.101) also means Information and Communication Technology (ICT).**

Information technology-related contracts **means those contracts that include services (including support services), and related resources for information technology.**

Organized health care arrangement **(see 45 CFR 160.103) means:**

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;

(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:

(i) Hold themselves out to the public as participating in a joint arrangement; and

(ii) Participate in joint activities that include at least one of the following:

(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement

and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or

(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

Privacy officer **means the HHS official(s) with responsibility for implementing and oversight of privacy related policies and practices that impact a given HHS acquisition.**

(b) ***General.*** **Contractors, subcontractors, their employees, third-parties, and business associates with access to HHS information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to the HHS Cybersecurity Program and the directives and handbooks, complete HHS security training prior to accessing HHS information (including HHS sensitive information and information systems security and privacy) and on an annual basis thereafter, as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, HHS** ***Personnel Security and Suitability Program*****, which establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards, and guidance for protecting HHS information, information systems (see 302.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.**

(c) ***Access to HHS information and HHS information systems.***

(1) Contractors are limited in their request for logical or physical access to HHS information or HHS information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery, or purchase orders.

(2) All Contractors, subcontractors, third parties, and business associates working with HHS information are subject to the same investigative requirements as those of HHS appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors to access HHS

information and HHS information systems shall be in accordance with HHS *Personnel Security and Suitability Program*.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling*" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be –

(i) Marked appropriately;

(ii) Disclosed to authorized personnel on a need-to-know basis;

(iii) Protected in accordance with NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and

(iv) Returned to HHS control, destroyed when no longer needed, or held until otherwise directed. Information and/or data must be disposed of in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

(5) *HIPAA business associate agreements*. Under the HIPAA Privacy and Security Rules (see 45 CFR 164), pursuant to 45 CFR 164.502(e)(1), a covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor of a covered entity's business associate. Additionally, a business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with 45 CFR 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information. The satisfactory assurances required by 45 CFR 45 CFR 164.504(e)(1) of this section shall be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of 45 CFR 164.504(e). The contracts shall also include breach reporting policies and procedures for suspected or confirmed breaches of protected health information. The contract shall impose a duty to cooperate with the

healthcare component and/or HHS breach investigation and response and must require all subcontractors to comply with the same HIPAA Rules requirements as a condition of receiving government data.

(i) ***Contractors or entities required to execute business associate agreements for contracts and other agreements become HHS business associates.*** **Business associate agreements are issued by HHS or may be issued by other HHS programs in support of HHS. The HIPAA Privacy Rule requires HHS to execute compliant business associate agreements with persons or entities that create, receive, maintain, or transmit HHS PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of HHS. There may be other HHS components or staff offices which also provide certain services and support to HHS and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to HHS, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a business associate agreements.**

(ii) ***Business associate agreement flow down to subcontractors.*** **A prime contractor required to execute a business associate agreement shall also obtain a satisfactory assurance, in the form of a business associate agreement, of its subcontractors who will also create, receive, maintain, or transmit PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA Rules requirements to the same degree as the Contractor. A contractor employing a subcontractor who creates, receives, maintains, or transmits PHI or that will store, generate, access, exchange, process, or utilize such PHI under a contract or agreement is required to execute a business associate agreement with each of its subcontractors which also obligates the subcontractor (*i.e.*, also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to PHI that is required of the covered entity and the prime contractor.**

(d) ***Contractor operations required to be in United States*****. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other HHS policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable business associate agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information System Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.**

(e) ***Roster of employees.*** **Contractors and subcontractors shall provide a roster containing the name, position, e-mail address, phone number, and responsibilities of each employee, including subcontractors, performing work under the contract to develop, have**

the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to Contracting Officer within _____[*Contracting Officer to insert the number of days*] days stated number of days from the effective date of the contract. Revisions to the roster as a result of staffing changes must be submitted within the number of days of the change provided by the Contracting Officer. The Contracting Officer, or the Contracting Officer's Representative (COR), will notify the Contractor of the appropriate level of investigation required for each staff member based on the information provided on the roster. If an employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.

(f) ***Contractor/subcontractor employee reassignment and termination notification*. Contractors and subcontractors shall provide written notification to the Contracting Officer and COR immediately, and not later than four (4) hours, when an employee working on an HHS information system or with access to HHS information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant HHS contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.**

(g) ***Non-disclosure agreement*. The Contractor and subcontractors shall submit completed non-disclosure agreements, as provided by the Contracting Officer, for each employee having access to non-public government information under this contract. The non-disclosure agreements shall be submitted to the Contracting Officer prior to the performance of work.**

(h) ***HHS information custodial requirements*. (1)** ***Release, publication, and use of data*. Information made available to a Contractor or subcontractor by HHS for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without HHS prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in 52.227-14, Rights in Data—General, paragraph (d).**

(2) ***Media sanitization*. HHS information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and HHS requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see HHS Cybersecurity Program). HHS reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and HHS requirements. The Contractor and subcontractor will provide all necessary access and support to HHS and/or GAO staff during periodic control assessments or audits.**

(3) *Data retention, destruction and contractor self-certification*. The Contactor and its subcontractors are responsible for collecting and destroying any HHS data provided, created, or stored under the terms of this contract, to a point where HHS data or materials are no longer readable or reconstructable to any degree, in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent directive. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction or return of all HHS data in its possession accordance with contract requirements or Contracting Officer instructions for disposition, including compliance with National Institute of Standards and Technology (NIST) SP 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) *Return of HHS data and information*. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the HHS (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying business associate agreement. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract using HHS-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information. No information, data, documentary material, records or equipment will be destroyed unless done in accordance with the terms of this contract and the HHS Agency Records Control Schedules (2019).

(5) *Use of HHS data and information*. The Contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of HHS information only in compliance with the terms of the contract and applicable Federal and HHS information confidentiality and security laws, regulations, and policies. If Federal or HHS information confidentiality and security laws, regulations, and policies become applicable to the HHS information or information systems after execution of the contract, or if the NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies for this contract as a result of any updates, if required.

(6) *Copying HHS data or information*. The Contractor/subcontractor shall not make copies of HHS information except as authorized and necessary to perform the terms of the contract or to preserve electronic information stored on Contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/subcontractor needs to be restored to an operating state. If copies are made

for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

(7) *Violation of information custodial requirements*. If HHS determines that the Contractor has violated any of HHS information confidentiality, privacy, or security provisions, it shall be sufficient grounds for HHS to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) *Encryption*. The Contractor/subcontractor must store, transport, or transmit HHS sensitive information, when permitted by the contract, using cryptography, HHS encryption policies, and HHS-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) *Firewall and web services security controls*. The Contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed HHS minimum requirements. HHS Configuration Standards Guidelines are available upon request.

(10) *Disclosure of HHS data and information*. Except for uses and disclosures of HHS information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose HHS information only in two other situations: (i) subject to paragraph 10 of this section, in response to a court order from a court of competent jurisdiction, or (ii) with HHS prior written approval. The Contractor/subcontractor must refer all requests for, demands for production of, or inquiries about, HHS information and information systems to the Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose HHS information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of HHS, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated HHS facility Privacy Officer as provided in the contract, business associate agreement, or by the Contracting Officer. If providing the Accounting of disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) *Compliance with privacy statutes and applicable regulations*. The Contractor/subcontractor shall not disclose HHS information protected by any of HHS privacy statutes or applicable regulations including, but not limited to, the Privacy Act of 1974 or the HIPAA Rules. If the Contractor/subcontractor is in receipt of a court order or other requests for HHS information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(i) *Compliance with identification policies*. Contractors shall comply with the Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; OMB M-19-17; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; HHS Policy for Information Security and Privacy Protection (IS2P) Control Catalog, and Executive Order 13467, Part 1, section 1.2.

(j) *Report of known or suspected incident or breach*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of a known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than _ days [*Fill in: Contracting Officer fills in the number of days*]. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (*e.g.*, Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within _____[*Fill in: Contracting Officer fills in the number of days in consultation with requiring activity*].

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–Security and Privacy Language.

(k) ***Incident and breach investigation*****. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.**

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(l) ***Incident and breach notification requirements*****. (1) The Contractor/subcontractor shall provide notice to HHS of an incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third-party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.**

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(m) *Training*. (1) All Contractor employees and subcontractor employees requiring access to HHS information or HHS information systems shall complete the following before being granted access to HHS information and its systems:

(i) On an annual basis, successfully complete the HHS Privacy and Information Security Awareness and HHS Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the HHS

Information Security Rules of Behavior, relating to access to HHS information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for HHS personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that HHS Information Security Rules of Behavior signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the HHS Information Security Rules of Behavior, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

(n) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and business associate agreements, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to HHS information (including HHS sensitive information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts.)

(End of clause)]

[352.204-72 Records management. (DEVIATION)

As prescribed in 304.7004, insert the following clause:

RECORDS MANAGEMENT (FEB 2024) (DEVIATION)

(a) *Applicability*. This clause applies to contracts that include Federal records, as defined in paragraph (b).

(b) *Definition.* As used in this clause—

***Federal record* means all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. See 44 U.S.C. 3301.**

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

(iii) Applies to records created, received, or maintained by Contractors pursuant to their contract; and

(iv) May include deliverables and documentation associated with deliverables.

(2) *Recorded information* means all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form. (See 44 U.S.C. 3301.)

(3) *Personal materials* means documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of Federal records and are not owned by the Government. (See 36 CFR 1220.18.)

(c) *Requirements.*

(1) The Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at 36 CFR chapter XII subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all Federal records, regardless of form or characteristics, mode of transmission, or state of completion.

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

(3) In accordance with 36 CFR 1222.32, the Contractor shall maintain all Federal records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the

provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

(5) The Contractor shall immediately notify the Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the contract. The Contractor shall ensure that appropriate personnel are trained to adhere to these contract requirements, and that applicable, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information, data, documentary material, Federal records and/or equipment is properly protected. The Contractor shall not remove Federal Records from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Contracting Officer. When information, data, documentary material, Federal records and/or equipment are no longer required, it shall be returned to HHS control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or as otherwise directed by the Contracting Officer. Destruction of Federal records is expressly prohibited unless in accordance with paragraph (c)(4).

(6) The Contractor shall only use Government information technology equipment for purposes specifically authorized by the contract and in accordance with HHS policy.

(7) The Contractor shall not create or maintain any Federal records containing any non-public HHS information that are not specifically authorized by the contract.

(8) The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

(9) All Contractor employees assigned to this contract handle Federal records are required to take HHS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

(d) *Subcontract flowdown.* The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract.]

*****

~~**352.224-70 Privacy Act.**~~**[(Deviation)]**

~~As prescribed in HHSAR 324.105(a), the Contracting Officer shall insert the following clause:~~

~~**Privacy Act (DEC 2015)**~~

~~This contract requires the Contractor to perform one or more of the following: (a) Design; (b) develop; or (c) operate a Federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) (5 U.S.C. 552a(m)(1)) and applicable agency regulations.~~

~~The term *system of records* means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties (5 U.S.C. 552a(i)).~~

~~The Contractor shall ensure that each of its employees knows the prescribed rules of conduct in 45 CFR part 5b and that each employee is aware that he/she is subject to criminal penalties for violation of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under this contract which require the design, development or operation of the designated system(s) of records (5 U.S.C. 552a(m)(1)). The contract work statement:~~

~~(a) Identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and~~

~~(b) Specifies the disposition to be made of such records upon completion of contract performance.~~

~~(End of clause)~~

[352.224-70 Notification of System of Records Notice. (Deviation)

As prescribed in 324.104(a), insert the following clause:

NOTIFICATION OF SYSTEM OF RECORDS NOTICE (FEB 2024) (DEVIATION)

(a) This contract provides for the design, development, or operation of a system of records about individuals from which information about an individual is retrieved by the individual's name or by some other identifying particular assigned to the individual.

(b) The System of Records Notice(s) (SORN(s)) that is applicable to this contract is/are: ___ ***[Contracting officer shall insert SORN name and number if one exists. If there is no SORN, indicate that a new or revised SORN will be developed].***

(c) The System of Records design, development, or operation work the Contractor is to perform is: _____*[Contracting officer shall insert description of design, development, and/or operation work to be performed; see definitions at FAR 24.101.].*

(d) The disposition to be made of the Privacy Act records upon completion of contract performance is as follows: _____*[Contracting*

officer shall insert records disposition instructions the contractor and any subcontractor must follow upon completion of contract performance].

(e) ***Subcontract flow down*****. The Contractor is required to include this clause in all subcontracts at any tier performing work under the prime contract involving design, development, or operation work involving a System of Records.**

(End of clause)]

352.224-71 Confidential Information. [(Deviation)]

As prescribed in ~~HHSAR~~ 324.105~~5~~**[4]**(b), insert the following clause:

CONFIDENTIAL INFORMATION (~~DEC 2015~~[FEB 2024]) [(DEVIATION)]

(a) **[*Definition*. As used in this clause—**

[*Confidential information]* ~~Confidential~~ **[i]** ~~Information, as used in this clause,~~ means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

(b) **[*Identification of information.*]** Specific **[confidential]** information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, ~~which are confidential may be~~ **[is]**identified ~~elsewhere~~ in this contract. ~~The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.~~

(c) **[*Disclosure.* The Contractor shall not disclose c]** ~~C~~onfidential **[i]** ~~I~~nformation or records ~~shall not be disclosed by the Contractor~~ until~~:(1)~~ **[w]** ~~W~~ritten ~~advance~~ notice **[is provided to the Contracting Officer]** ~~of~~ at least 45 days **[in advance]** ~~shall be provided to the Contracting Officer~~ of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.**[The Contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.]**

(~~2~~**[(d)]**) **[*Government furnished or provided information:*** For information provided by or on behalf of the government—

(~~i~~**[1]**) The publication or dissemination of the following types of information are restricted under this contract: _____[**[*Contracting Officer to insert restricted types of information, If none, so state.*]**] ~~INSERT RESTRICTED TYPES OF INFORMATION. If none, so state.]~~

(~~ii~~**[2]**) The reason(s) for restricting the types of information identified in subparagraph **[(d)(1)]**~~(i)~~ is/are: _____[**[*Contracting Officer to state why the***

public or Government interest requires the restriction of each type of information identified. Any basis for nondisclosure which would be valid under the Freedom of Information Act is sufficient under this clause.]] ~~STATE WHY THE PUBLIC OR GOVERNMENT INTEREST REQUIRES THE RESTRICTION OF EACH TYPE OF INFORMATION. ANY BASIS FOR NONDISCLOSURE WHICH WOULD BE VALID UNDER THE FREEDOM OF INFORMATION ACT IS SUFFICIENT UNDER THIS CLAUSE.]~~

~~(iii) Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.~~

(~~d~~**[e]**) ~~Whenever t~~**[T]**he Contractor **[shall consult with the Contracting Officer when there is uncertainty]**~~is uncertain~~ with regard to the confidentiality of**[,]** or a property interest in**[,]** information under this contract~~, the Contractor should consult with the Contracting Officer~~ prior to **[the]**~~any~~ release, disclosure, dissemination, or publication**[of such information]**.

[(End of clause)]

*** * * * ***

[352.239-71 Security Requirements for Information Technology Resources. (Deviation)

As prescribed in 339.106-70(a), insert the following clause:

SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (FEB 2024) (DEVIATION)

(a) ***Definitions*****. As used in this clause—**

Information technology **has the same meaning in FAR 2.101.**

Information and communication technology (ICT) also means **information technology (see FAR 2.101 for definitions).**

Information system security plan **means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.**

(b) ***Responsibilities*****. The Contractor shall be responsible for information technology security for all systems connected to a Department of Health and Human Services (HHS) network or operated by the Contractor for HHS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to HHS information that directly supports the mission of HHS. Examples of tasks that require security provisions include—**

(1) Hosting of HHS e-Government sites or other information technology operations;

(2) Acquisition, transmission, or analysis of data owned by HHS with significant replacement cost should the contractor's copy be corrupted; and

(3) Access to HHS general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.

(c) ***Information system security plan*****. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. HHS information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting those requirements. Generally, this plan shall describe the processes and procedures that the Contractor will follow to ensure appropriate security of information system resources developed, processed, or used under this contract. The security plan should include implementation status, responsible entities, resources, and estimated completion dates. Security plans may also include, but are not limited to, a**

compiled list of system characteristics or qualities required for system registration, and key security-related documents such as a risk assessment, privacy impact assessment (PIA), system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and the system privacy plan, as determined by the Contracting Officer's Representative. The plan shall address the specific contract requirements regarding information systems or related support or services included in the contract, to include the PWS or SOW. The Contractor's Information System Security Plan shall comply with applicable Federal Laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Modernization Act (FISMA) of 2014 and the E-Government Act of 2002. The plan shall meet information technology security requirements in accordance with Federal and HHS policies and procedures, and as amended during the term of this contract, and include, but are not limited to the following:

(1) OMB Circular A-130, Managing Information as a Strategic Resource;

(2) National Institute of Standards and Technology (NIST) Guidelines;

(3) Federal Information Processing Standard (FIPS) 200; and

(4) HHS Cybersecurity Program related to HHS information (including HHS sensitive information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, the Cyber Security Checklist and Cyber Security Infographic at https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html, which provides HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting HHS information, information systems (see 302.101, Definitions), information technology, and ICT, security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.

(d) *Submittal of plan*. Within 60 days after contract award, the Contractor shall submit the Information System Security Plan to the Contracting Officer for review and approval.

(e) *Authority to Operate (ATO)*. As required by current HHS policy, the Contractor shall submit written proof of information technology security accreditation with a valid ATO to the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. Accreditation shall be in accordance with HHS policy available from the Contracting Officer upon request. The Contractor shall submit for acceptance by the Contracting Officer along with this ATO a final security plan, risk assessment, security test and evaluation, privacy threshold analysis or privacy impact assessment, and a disaster recovery plan/continuity of operations plan.

(f) *Annual validation*. On an annual basis, the Contractor shall verify in writing to the Contracting Officer that the IT Security Plan remains valid.

(g) *Banners*. The Contractor shall ensure that the official HHS banners are displayed on all HHS systems (both public and private) operated by the Contractor that contain Privacy Act or other sensitive information before allowing anyone access to the system. The Office of Information Technology will make official HHS banners available to the Contractor.

(h) *Screening and access*. The Contractor shall screen all personnel requiring privileged access or limited privileged access to systems operated by the Contractor for HHS or interconnected to an HHS network in accordance with HHS policies referenced in paragraph (c).

(i) *Training*. The Contractor shall ensure that its employees performing services under this contract complete HHS security awareness and privacy training on an annual basis. This includes signing an acknowledgment on an annual basis that they have read, understand, and agree to abide by the HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy as required; FAR 39.105, Privacy; clause 352.204-71, Information and Information Systems Security, and this clause.

(j) *Government access*. The Contractor shall provide the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, information systems, databases, and personnel used in performance of the contract. The Contractor shall provide access to enable a program of information technology inspection (to include vulnerability testing), investigation and audit (to safeguard against threats and hazards to the integrity, availability and confidentiality of HHS data or to the function of information technology systems operated on behalf of HHS), and to preserve evidence of computer crime.

(k) *Notification of termination of employees*. The Contractor shall immediately notify the Contracting Officer when an employee who has access to HHS information systems or data terminates employment.

(l) *Subcontract flow down requirement*. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts that meet the conditions in paragraph (a) of this clause.

(End of clause)

352.239-72 Information System Security Plan and Accreditation. (Deviation)

As prescribed in 339.106-70(a), insert the following provision:

INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2024) (DEVIATION)

All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 352.239-71, Security Requirements for Information Technology Resources.

(End of provision)

352.239-73 Information System Design and Development. (Deviation)

As prescribed in 339.106-70(b), insert the following clause:

INFORMATION SYSTEM DESIGN AND DEVELOPMENT (FEB 2024) (DEVIATION)

(a) ***Design or development at non-HHS facilities*****. Information systems that are designed or developed for or on behalf of HHS at non-HHS facilities shall comply with all HHS directives developed in accordance with the Federal Information Security Modernization Act of 2014, Health Insurance Portability and Accountability Act (HIPAA) regulations, National Institute of Standards and Technology (NIST), and related HHS security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic protected health information (PHI), outlined in 45 CFR Part 164, Subpart C, information and system security categorization level designations in accordance with Federal Information Processing Standards (FIPS) 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization and the Trusted Internet Connections Reference Architecture.**

(b) ***Privacy Impact Assessment*****. During the development cycle a Privacy Impact Assessment must be completed by the contractor, provided to the Contracting Officer Representative, and approved by the appropriate HHS and Operating Division security and privacy officials; government, contractor, or independent third party.**

(c) ***Security of procured or developed systems and technologies*****. The Contractor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of the contract and any extension, warranty, or maintenance periods. This includes, but is not limited to, workarounds, patches, hotfixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the Contractor anywhere in the Systems, including Operating Systems and firmware. The Contractor shall ensure that security fixes shall not negatively impact the Systems.**

(d) *Subcontract flow down requirements*. The Contractor shall incorporate and flow down the substance of this clause to all subcontracts where services to perform information system design and development are required.

(End of clause)

352.239-74 Information System Hosting, Operation, Maintenance, or Use. (Deviation)

As prescribed in 339.106-70(c), insert the following clause:

INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE (FEB 2024) (DEVIATION)

(a) *Definitions*. As used in this clause—

***Assessment and Authorization* (A&A) means the process used to ensure information systems including Major Applications and General Support Systems have effective security safeguards which have been implemented, planned for, and documented in an Information Technology Security Plan. The A&A process per applicable HHS policies and procedures is the mechanism by which HHS provides an Authorization to Operate (ATO), the official management decision given by the HHS to authorize operation of an information system.**

***Information system security plan* means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.**

(b) *Hosting, operation, maintenance, or use at non-HHS facilities*. For information systems that are hosted, operated, maintained, or used on behalf of HHS at non-HHS facilities, Contractors/subcontractors are fully responsible and accountable for ensuring compliance with all applicable Health Insurance Portability and Accountability (HIPAA) Act of 1996 (HIPAA) regulations, the Privacy Act and other required HHS confidentiality statutes included in HHS mandatory yearly training and privacy policy, Federal Information Security Modernization Act (FISMA), National Institutes of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), and HHS security and privacy policy. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security and privacy control procedures must be equivalent to or exceed, those procedures used to secure HHS systems. A Privacy Impact Assessment (PIA) (if the system includes Personally Identifiable Information (PII)) or a Privacy Threshold Analysis (to determine if the system includes PII) must also be provided to the Contracting Officer Representative (COR) and approved by HHS Senior Agency Official for Privacy (SAOP) or designee prior to ATO. All external Internet connections to HHS network involving HHS information must be in accordance with the Trusted Internet Connections (TIC) Reference Architecture and

reviewed and approved by HHS prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

(c) ***Collecting, processing, transmitting, and storing of PII*****. Adequate security and privacy controls for collecting, processing, transmitting, and storing of PII, as determined by the HHS SAOP or designee, must be in place, tested, and approved by HHS prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of HHS. These security and privacy controls are to be assessed and stated within the PIA, Information System Security Plan, Information System Privacy Plan, Security Control Assessment Report, and/or Privacy Control Assessment Report, as agreed upon by the Contractor, COR, and the Operating Division Senior Official for Privacy. If these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.**

(d) ***Annual FISMA security controls assessment*****. The Contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the Contracting Officer for entry into HHS Plan of Action & Milestones (POA&M) management process. The Contractor/subcontractor must use HHS POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes specified by the HHS in the performance work statement or statement of work, or in the approved remediation plan through the HHS POA&M process. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by HHS officials, including the HHS Office of Inspector General. The physical security aspects associated with Contractor/subcontractor activities must also be subject to such assessments. The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per HHS Rules of Behavior for the Use of HHS Information and IT Resources Policy. Major changes introducing new privacy risks require an updated and reapproved PIA.**

(e) ***Annual self-assessment*****. The Contractor/subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. HHS reserves the right to conduct such an assessment using government personnel or another Contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action, as may be specifically addressed in the contract, to correct or mitigate any weaknesses discovered during such testing, at no additional cost to the Government to correct Contractor/subcontractor systems and outsourced services.**

(f) ***Prohibition of installation and use of personally-owned or Contractor-owned equipment or software on HHS networks*****. HHS prohibits the installation and use of**

personally-owned or Contractor/subcontractor-owned equipment or software on HHS networks. If non-HHS owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, performance work statement, statement of work, or contract. All of the security controls required for government furnished equipment must also be utilized in approved other equipment (OE) at the Contractor's expense. All remote systems must be equipped with, and use, an HHS-approved antivirus software and a personal (host-based or enclave based) firewall that is configured with an HHS-approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-HHS owned OE.

(g) ***Disposal or return of electronic storage media on non-HHS leased or non-HHS owned IT equipment.*** **All electronic storage media used on non-HHS leased or non-HHS owned IT equipment that is used to store, process, or access HHS information must be handled in adherence with disposition instructions upon—**

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier. Media (*e.g.*, hard drives, optical disks, CDs, back-up tapes) used by the Contractors/ subcontractors that contain HHS information must be returned to the HHS for sanitization or destruction or the Contractor/subcontractor must self-certify that the media has been disposed of per disposition instructions. This must be completed within 30 days of termination of the contract.

(h) ***Bio-Medical devices and other equipment or systems*****. Bio-Medical devices and other equipment or systems containing media (*e.g.*, hard drives, optical disks) with HHS sensitive information will not be returned to the Contractor at the end of lease, for trade-in, or other purposes. For purposes of these devices and protection of HHS sensitive information the devices may be provided back to the Contractor under one of three scenarios—**

(1) The Contractor must accept the system without the drive;

(2) A spare drive must be installed in place of the original drive at time of turn-in if HHS initial medical device purchase included a spare drive; or

(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

352.239-75 Security Controls Compliance Testing. (Deviation)

As prescribed in 339.106-70(d), insert the following clause:

SECURITY CONTROLS COMPLIANCE TESTING (FEB 2024) (DEVIATION)

On a periodic basis, HHS, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy controls implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein HHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of HHS, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice, to include unannounced assessments, as determined by HHS in the event of an incident or a breach, or at any other time.

(End of clause)

352.239-76 Security Requirements for Government-Owned Contractor-Operated and Contractor-Owned Contractor-Operated Resources. (Deviation)

As prescribed in 339.106-70(e), insert the following clause:

SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED CONTRACTOR-OPERATED AND CONTRACTOR-OWNED CONTRACTOR-OPERATED RESOURCES (FEB 2024) (DEVIATION)

(a) *Federal policies*. The Contractor shall comply with applicable federal laws, regulations, and HHS policies that include, but are not limited to—

(1) HHS Policy for Information Security and Privacy Protection (IS2P);

(2) Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101);

(3) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, Security and Privacy Controls for Information Systems and Organizations;

(4) Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource; and

(5) Any other applicable federal laws, regulations, NIST guidance, and local HHS policies.

(b) *Assessment and Authorization (A&A).* A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the

Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) of _____ *[Contracting Officer insert timeline(s)]*. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/*_____ *[Contracting Officer insert other policies, if applicable]*, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision). HHS acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

(1) *A&A package deliverables.* The Contractor shall provide an A&A package within _____ *[Contracting Officer insert required timeline, process, and format for A&A package delivery or indicate timeline/format for each individual deliverable]* to the Contracting Officer and/or the Contracting Officer's Representative (COR). The following A&A deliverables are required to complete the A&A package—

(i) _____ *[Contracting Officer insert specific deliverables, as applicable, in addition to the HHS baseline listed below]*:

(ii) A System Security Plan (SSP) is due _____ *[Contracting Officer insert specific timeline, process, and format for deliverable]*. 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 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 policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system (see HHSAR 302.101, Definitions) 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 review and update the SSP at least annually thereafter and if requested, provide a copy of the updated SSP to the COR.

(iii) A Security Assessment Plan/Report (SAP/SAR) is due _____ [*Contracting Officer insert specific timeline, process and format for deliverable].* The security assessment must be conducted by *[Contracting Officer include type of assessment (e.g., independent, etc.)]* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with the COR shall conduct, or as directed, in the assessment of the security controls _____ [*Contracting Officer insert specific timeline(s), if applicable*] and update the SAR at least annually. A copy of the updated SAR shall be provided to the COR, if requested.

(iv) All systems shall have a completed privacy threshold analysis (PTA). If the PTA results determines the system contains personally identifiable information, a privacy impact assessment, approved by the HHS SAOP, is required.

(v) System Privacy Plan and Privacy Control Assessment. As required in OMB Circular A-130, a System Privacy Plan and Privacy Control Assessment shall be included in A&A. The plan and assessment may be included in the Security System Plan, or a separate report in the A&A, as determined by the COR.

(vi) An Independent Assessment is due _____[*Contracting Officer insert specific timeline, process, and format for the deliverable].* The Contractor shall have an independent third-party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party 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 _____[*Contracting Officer insert all other deficiencies that may require mitigation by Contractor*] before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).

(vii) The POA&M is due as follows—

(A) _____[*Contracting Officer insert specific overall timeline, process, and format for the deliverable*] from the date the weaknesses are formally identified and documented;

(B) Critical-risk weaknesses must be mitigated within _____ [*Contracting Officer insert specific timeline*] from the date the weaknesses are formally identified and documented;

(C) High-risk weaknesses must be mitigated within _____ [*Contracting Officer insert specific timeline*] from the date the weaknesses are formally identified and documented;

(D) Medium weaknesses must be mitigated within _____ [*Contracting Officer insert specific timeline*] from the date the weaknesses are formally identified and documented; and

(E) Low weaknesses must be mitigated within _____ [*Contracting Officer insert specific timeline*], from the date the weaknesses are formally identified and documented.

(2) HHS will determine the risk rating of all vulnerabilities. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defect in a system (that require to create a patch for remediation), and other security reviews and

sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones policies. Depending on the severity of the risks, HHS may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document shall be updated at least quarterly _____[*Contracting Officer insert timeline, process, and format if more frequent updates are needed*].

(3) A Contingency Plan and Contingency Plan Test are due _____ [*Contracting Officer insert specific timeline, process and format for the deliverable*]. The Contingency Plan shall be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS policies. Upon final acceptance by the System Owner, the Contractor, in coordination with the COR and System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned, and any remaining action items to be addressed. The Contractor shall update and test the Contingency Plan at least *annually*.

(4) An E-Authentication Questionnaire is required. The Contractor shall collaborate with at the COR's direction to ensure that the E-Authentication Guidance requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 series, latest versions. Based on the level of assurance determined by the E-Authentication, the Contractor shall ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Authentication (when required), in accordance with HHS *Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS policies.

(5) *Information security continuous monitoring.* Upon the government issuance of an ATO, the Contractor-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*, HHS ISCM Strategy, and HHS IS2P.

(6) *Annual assessment/penetration (pen) test*. The Contractor shall assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the agency or independent third-party _____ [*Contracting Officer insert pen test requirement, if needed*].) In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by the specified due date provided by the COR.

(7) *Asset management.* Using any available Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, the Contractor shall 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 and/or data. It is anticipated that this inventory information will be required to be produced at least _____[*Contracting Officer insert specific timeframe*]. IT asset inventory information shall include—

(i) IP address;

(ii) Machine name;

(iii) Operating system level;

(iv) Security patch level; and

(v) 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 in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS policy.

(8) *Configuration management*. The Contractor shall use available SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to computers, servers, routers, databases, operating systems, application, etc., that store and process government information. The Contractor shall provide scan reports to the COR upon request. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

(9) *Vulnerability management.* The Contractor shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor 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 _____[*Contracting Officer insert specific timeframe*].

(10) *Patching and vulnerability remediation*. The Contractor shall 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.

(11) *Secure coding.* The Contractor shall follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team specified standards, the Software Engineering Institute (SEI) CERT and the Open Web Application Security Project, that will limit system software vulnerability exploits.

(12) *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.

(13) *Government access for security assessment.*

(i) In addition to the Inspection Clause in the contract, the Contractor 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. This access includes, but is not limited to—

(1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, access to 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. For the purposes of this paragraph only, *Government* includes, but is not limited to, Contracting Officer, COR, the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of 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, Structured Query Language injection vulnerabilities, and any other known vulnerabilities.

(2) At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

(ii) The Contractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Government inspectors, auditors, and

investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

(iii) The Contractor shall cooperate with inspections, audits, investigations, and reviews.

(c) *End of Life compliance*. The Contractor shall use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the OPDIV CISO if it impacts only the OPDIV). The contractor must retire and/or upgrade all software/systems that have reached end-of-life in accordance with *HHS End of Life Operating Systems, Software and Application Policy*.

(d) *Desktops, laptops, and other computing devices required for use by the Contractor.* The Contractor 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:

(1) Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program.

(2) Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline, _____ [*Contracting Officer insert specific security configuration baseline, if applicable*], and HHS Minimum Security Configuration Standards;

(3) Maintain the latest operating system patch release and anti-virus software definitions at least _____[*Contracting Officer, insert specific timeline(s)*];

(4) Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

(5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:

(i) Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and

(ii) Using SCAP-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the Contracting Officer and/or

COR, Project Officer, and any other point of contract designated by the Contracting Officer or COR.

(e) ***Rights to data.*** **Contractors shall specify any data rights asserted and mark such deliverables accordingly in accordance with applicable data rights clauses set forth in the contract.**

(f) ***Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements*****. The Contractor shall secure their ICT supply chain in compliance with** ***HHS Policy for Cyber Supply Chain Risk Management*** **and Public Law 115-232, section 889. At a minimum, the Contractor shall—**

(1) Develop rules for suppliers' development methods, techniques, or practices;

(2) Use secondary market components;

(3) Prohibit counterfeit products;

(4) Dispose and/or retain elements such as components, data, or intellectual property securely;

(5) Ensure adequate supply of components;

(6) Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;

(7) Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;

(8) Establish Service Level Agreements (SLAs), patching vehicles, and disclosure requirements in the case of an incident or new vulnerability being discovered; and

(9) Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and

(10) Prohibit the use of covered telecommunications and video surveillance equipment or services.

(g) ***Subcontract flow down*****. The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts and third-party agreements, at any tier, of any amount and in which subcontractor employees and third-party servicers/employees, will perform functions or provide products under the scope of this contract, and have access to HHS information (including HHS sensitive information,** ***i.e.*****, protected health**

information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101, Definitions).

(End of clause)

352.239-77 Cloud Computing Services. (Deviation)

As prescribed in 339.106-70(f), insert the following clause:

CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION)

(a) *Responsibilities.* This clause is applicable to all or any part of the contract that includes cloud computing services. The Contractor shall be responsible for the following privacy and security requirements on this contract—

(1) *Federal Risk and Authorization Management Program (FedRAMP) compliant authorization to operate.* Compliance with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service (see HHSAR 302.101, Definitions) under this contract has an approved FedRAMP compliant authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by _____[*Contracting Officer to insert specific timeframe, process and format for Contractor to submit ATO package and/or deliverables*].

(i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at fedramp.gov). The *HHS Policy for Information Security and Privacy Protection (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 implement additional controls identified by the agency in this contract.

(ii) A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter, or when 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, when applicable ___[*Contracting Officer to insert locations and boundaries*].

(3) *Service Level Agreements (SLAs).* When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between

cloud customers and the cloud service provider and work with the Contracting Officer's Representative (COR) to develop and maintain an SLA, as provided in the contract.

(4) *Interconnection Agreements/Memorandum of Agreements.* When applicable and identified in this contract, the Contractor shall establish and maintain interconnection agreements and or memorandum of agreements/understanding in accordance with HHS policies.

(b) *Protection of information in a cloud environment.*

(1) If Contractor personnel shall 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 policies, available at https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html.

(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 shall be made available to HHS, at no additional cost, within one (1) business day from the date of the request, or within the timeframe otherwise specified.

(3) The Contractor 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 comply with NARA-approved records schedule(s) and protection requirements for federal agency electronic records in accordance with 36 CFR 1236.20 and 1236.22 (ref. a), including but not limited to —

(i) Maintenance of links between records and metadata; and

(ii) 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 the COR. 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.

(i) 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 _____ [*Contracting Officer insert necessary Privacy Act language required, or reference location*].

(c) ***Assessment and Authorization (A&A) process.***

(1) The Contractor shall comply with HHS and FedRAMP requirements as mandated by federal laws, regulations, privacy policies, and HHS policies, including making available any documentation, physical access, and logical access needed to support the A&A requirement. The level of effort for the A&A is based on the system's FIPS 199 security categorization and HHS security policies.

_____ [*Contracting Officer insert certification timeframe***].**

(i) In addition to the FedRAMP compliant ATO, the Contractor shall complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation _____ [*Contracting Officer insert additional language, as applicable, to include completion/submission timelines***]. The agency ATO must be approved by the HHS authorizing official (AO) prior to implementation of system and/or service being acquired.**

(ii) Cloud Service Provider (CSP) systems categorized as FIPS 199 High, Moderate or Low are recommended but not required to leverage a FedRAMP accredited Third Party Assessment Organization (3PAO). A CSP's agency partner may choose to use their own Independent Verification and Validation (IV&V) organization or 3PAO to assess the system. If an agency chooses to use their own IV&V team or an unaccredited 3PAO, they must submit an attestation regarding the team's independence to the agency and the FedRAMP PMO, and the IV&V / 3PAO team must use FedRAMP templates for the assessment and follow all FedRAMP requirements.

(iii) For all cloud services, the A&A package must contain the following documentation:

_____
[*Contracting Officer insert appropriate A&A package deliverables***].**

(iv) Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with HHS policies. The following templates and timelines are applicable.

_____
[*Contracting Officer insert required deliverable templates and timelines***].**

(2) HHS reserves the right to perform penetration testing on all systems operated on behalf of the agency. If the Contracting Officer exercises this right, the Contractor 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—

(i) Scanning operating systems, web applications, wireless scanning;

(ii) Network device scanning to include routers, switches, and firewall, and IDS/IPS; and,

(iii) 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 shall identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, HHS may require remediation at the Contractor's expense before HHS issues an ATO.

(4) The Contractor shall mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings shall be remediated in accordance with timelines specified in the HHS POA&M Standard from discovery—

(i) Critical vulnerabilities no later than fifteen (15) days;

(ii) High within thirty (30) days;

(iii) Medium within ninety (90) days; and

(iv) Low vulnerabilities no later than three hundred and sixty (360) days, unless otherwise specified.

(v) In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the newly designated timelines _____[*Contracting Officer insert timelines for mitigating POA&M weaknesses*]. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

(5) Revocation of a cloud service. HHS has 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 (see HHSAR 302.101, Definitions), HHS 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 Contracting Officer 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, other networks, or applying additional security controls.

(d) ***Reporting and continuous monitoring.***

(1) Following the initial ATOs, the Contractor shall perform the minimum ongoing continuous monitoring activities, 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. The minimum ongoing continuous monitoring activities include—

_____[*Contracting Officer insert meeting/deliverable timelines as necessary; applicable Continuous Monitoring requirements, and approved CSP specific Continuous Monitoring Plan requirements***].**

(2) At a minimum, the Contractor shall provide the following artifacts/deliverables on a monthly basis—

_____[*Contracting Officer insert process and format for deliverables***]:**

(i) Operating system, database, Web application, and network vulnerability scan results;

(ii) Updated POA&Ms;

(iii) Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the System Owner or AO, and;

(iv) Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS 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 shall 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 *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS _____[*Contracting Officer insert Specific configuration requirements***] configuration baseline.**

(2) The Contractor shall use NIST 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) *Report of known or suspected incident or breach*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the Contracting Officer and the COR or within one (1) hour of an known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than _ days [*Fill in: Contracting Officer fills in the number of days*]. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (*e.g.*, Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to HHS that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within _____[*Fill in: Contracting Officer fills in the number of days in consultation with requiring activity*].

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, in accordance with the timelines specified in the HHS Policy for Vulnerability Management, and the HHS Standard for Plan of Action and Milestones (POAM) Management and Reporting. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of HHS) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the Office of the Chief Information Officer (OCIO). These exceptions will be tracked by the Contractor in concert with the Government in accordance with HHS Policy for IT Procurements–- Security and Privacy Language.

(g) *Incident and breach investigation*. (1) The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected incident or breach (see definitions, paragraph (a)), or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(2) To the extent known by the Contractor/subcontractor, the Contractor/ subcontractor's notice to HHS shall identify the information involved, an estimate of the number of potentially impacted individuals, the circumstances surrounding the incident (including to whom, how, when, and where the HHS information or assets were placed at risk or compromised), and any other information that the Contractor/subcontractor considers relevant.

(3) With respect to unsecured protected health information, the business associate is deemed to have discovered an incident as defined above when the business associate either knew, or by exercising reasonable diligence should have been known to an employee of the business associate. Upon discovery, the business associate must notify HHS of the incident immediately within one hour of discovery or suspicion as agreed to in the business associate agreement.

(4) In instances of theft or break-in or other criminal activity, the Contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction. The Contractor, its employees, and its subcontractors and their employees shall cooperate with HHS and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/subcontractor shall cooperate with HHS in any civil litigation to recover HHS information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

(h) ***Incident and breach notification requirements*****. (1) The Contractor/subcontractor shall provide notice to HHS of a privacy or incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third-party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.**

(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including:

(A) Date of occurrence.

(B) Date of incident or breach detection.

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of HHS control.

(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(i) ***Media transport.***

(1) The Contractor 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).

_____[*Contracting Officer insert minimum requirements***].**

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

(j) ***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 TIC processes that are in compliance with the requirements of the Office of Management and Budget Memorandum 19-26: Update to the TIC Initiative, TIC 3.0.

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

(3) Non-Repudiation. The Contractor shall provide a system that implements encryption with current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program that provides for origin authentication, data integrity, and signer non-repudiation.

(k) ***Subcontract flow down*****. The Contractor shall include the substance of this clause, including this paragraph (i), in subcontracts and third-party agreements, of any amount and in which subcontractor employees, and third-party servicers/employees, will perform functions where they will provide cloud computing services and have access to HHS information (including HHS sensitive information, *i.e.*, protected health information (see HHSAR 302.101, Definitions)), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101 definition of information technology-related contracts).**

(End of clause)]

352.239-7~~3~~[8] ~~Electronic~~ Information and [Communication]Technology Accessibility Notice. [(Deviation)]

~~(a)~~ As prescribed in 339.203-70(a), ~~the Contracting Officer shall~~ insert the following provision:

~~Electronic and Information Technology Accessibility Notice~~[INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE] (~~DEC 2015~~[FEB 2024]) [(DEVIATION)]

[(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

~~(b)~~ The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-79 Information and Communication Technology Accessibility. In order to facilitate the Government's determination whether proposed ICT supplies, products, platforms, information, and documentation meet applicable Section 508 accessibility standards, offerors must submit an appropriate HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), in accordance with the completion instructions. The purpose of the checklists and conformance reports are to assist HHS acquisition and program officials in determining whether proposed ICT supplies, products, platforms, information, and documentation conform to applicable Section 508 accessibility standards. Checklists and ACRs evaluate—in detail—whether the ICT conforms to specific

Section 508 accessibility standards and identifies remediation efforts needed to address conformance issues.

~~(c)~~ If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of a contract or order, that supplies, products, platforms, information, documentation, or services support delivered do not conform to the described accessibility standards, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

~~(d)~~ In order to facilitate the Government's determination whether proposed ICT supplies meet applicable Section 508 accessibility standards, offerors must submit an Accessibility Conformance Report, in accordance with its completion instructions and tailored to the requirements in the solicitation. The purpose of the Report is to assist HHS acquisition and program officials in determining whether proposed ICT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document, in detail, whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available at https://Section508.gov/.

~~(e)~~ In order to facilitate the Government's determination whether proposed ICT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the ICT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.

~~(f)~~ Respondents to this solicitation must identify any inability to conform to Section 508 requirements. If an offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, i.e., after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.

~~(g)~~ Items delivered as electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at http://508.hhs.gov/. Materials, other than items incidental to contract management, that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Contracting Officer's Representative.

(End of provision)]

~~the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 and the Architectural and Transportation Barriers Compliance Board Electronic and Information (EIT) Accessibility Standards (36 CFR part 1194), require that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal~~

~~employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.~~

~~(b) Accordingly, any offeror responding to this solicitation must comply with established HHS EIT accessibility standards. Information about Section 508 is available at *http://www.hhs.gov/web/508*. The complete text of the Section 508 Final Provisions can be accessed at *http://www.access-board.gov/guidelines-and-standards/communications-and-…*.~~

~~(c) The Section 508 accessibility standards applicable to this solicitation are stated in the clause at 352.239-74, Electronic and Information Technology Accessibility.~~

~~In order to facilitate the Government's determination whether proposed EIT supplies meet applicable Section 508 accessibility standards, offerors must submit an HHS Section 508 Product Assessment Template, in accordance with its completion instructions. The purpose of the template is to assist HHS acquisition and program officials in determining whether proposed EIT supplies conform to applicable Section 508 accessibility standards. The template allows offerors or developers to self-evaluate their supplies and document - in detail - whether they conform to a specific Section 508 accessibility standard, and any underway remediation efforts addressing conformance issues. Instructions for preparing the HHS Section 508 Evaluation Template are available under Section 508 policy on the HHS Web site *http://www.hhs.gov/web/508*.~~

~~In order to facilitate the Government's determination whether proposed EIT services meet applicable Section 508 accessibility standards, offerors must provide enough information to assist the Government in determining that the EIT services conform to Section 508 accessibility standards, including any underway remediation efforts addressing conformance issues.~~

~~(d) Respondents to this solicitation must identify any exception to Section 508 requirements. If a offeror claims its supplies or services meet applicable Section 508 accessibility standards, and it is later determined by the Government, *i.e.*, after award of a contract or order, that supplies or services delivered do not conform to the described accessibility standards, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its expense.~~

~~(End of provision)~~

352.239-74[9] ~~Electronic and~~ Information [and Communication] Technology Accessibility. [(Deviation)]

As prescribed in 339.203-70(b), insert the following clause:

~~Electronic and Information Technology Accessibility~~[INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY] (~~DEC 2015~~[FEB 2024]) [(DEVIATION)]

[(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services

support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.

(b) Additional Section 508 accessibility standards applicable to this contract or order may be identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies or services conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(d) If this is an Indefinite-Delivery type contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include ICT supplies, products, platforms, information, documentation, or services support will define the specifications and accessibility standards for the order. In those cases, the Contractor shall be required to provide a completed HHS Section 508 Accessibility Conformance Checklist (see *https://www.hhs.gov/web/section-508/accessibility-checklists/index.html*) or an ACR (based on the VPAT see https://www.itic.org/policy/accessibility/vpat), and any other additional information necessary to assist the Government in determining that the ICT supplies, products, platforms, information, documentation, or services support conform to Section 508 accessibility standards. If it is determined by the Government that ICT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) The contractor shall identify to the Contracting Officer any perceived exception or exemption to Section 508 requirements.

(End of clause)]

(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all electronic and information technology (EIT) supplies and services developed, acquired, or maintained under this contract or order must comply with the "Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR part 1194. Information about Section 508 is available at *http://www.hhs.gov/web/508*. The complete text of Section 508 Final Provisions can be accessed at *http://www.access-board.gov/guidelines-and-standards/communications-and…*. -

(b) The Section 508 accessibility standards applicable to this contract or order are identified in the Statement of Work or Specification or Performance Work Statement. The contractor must provide any necessary updates to the submitted HHS Product Assessment Template(s) at the end of each contract or order exceeding the simplified acquisition threshold (see FAR 2.101) when the contract or order duration is one year or less. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) The Section 508 accessibility standards applicable to this contract are:

(Contract staff must list applicable standards)

(d) In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS Web site: (*http://www.hhs.gov/web/508*). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(e) If this is an Indefinite Delivery contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include EIT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found at *http://www.hhs.gov/web/508*. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the

~~provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.~~

~~(End of clause)~~