

SOLICITATION, OFFER AND AWARD		1. This Contract is a Rated Order under the Defense Priorities and Allocations System (DPAS) - Code of Federal Regulations - at 15 CFR 700.		RATING	PAGE OF PAGES 1 107		
2. CONTRACT NUMBER		3. SOLICITATION NUMBER 75F40126R00009		4. TYPE OF SOLICITATION ☐ SEALED BID (IFB) INVITATION FOR BID ☒ NEGOTIATED (RFP) REQUEST FOR PROPOSAL		5. DATE ISSUED 09/04/2026	6. REQUISITION/PURCHASE NUMBER
7. ISSUED BY DHHS/FDA/OAGS/DAO 11601 Landsdown St. 13th Floor North Bethesda MD 20852		CODE DAO		8. ADDRESS OFFER TO (If other than Item 7)			

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION	
9. Sealed offers in original and _____ copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if hand carried, in the depository located in _____ until <u>1400 ET</u> local time <u>09/21/2026</u> (Hour) (Date)	
CAUTION: LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.	
10. FOR INFORMATION CALL:	A. NAME MELINDA KIM B. TELEPHONE (NO COLLECT CALLS) AREA CODE 301 NUMBER 796-0607 EXT. C. E-MAIL ADDRESS MELINDA.KIM@FDA.HHS.GOV

11. TABLE OF CONTENTS							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
☒	A	SOLICITATION/CONTRACT FORM	1-3	☒	I	CONTRACT CLAUSES	51-84
☒	B	SUPPLIES OR SERVICES AND PRICES/COSTS	4	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS			
☒	C	DESCRIPTION/SPECIFICATIONS/WORK STATEMENT	5-27	☒	J	LIST OF ATTACHMENTS	85
☒	D	PACKAGING AND MARKING	28	PART IV - REPRESENTATIONS AND INSTRUCTIONS			
☒	E	INSPECTION AND ACCEPTANCE	29	☒	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	86-90
☒	F	DELIVERIES OR PERFORMANCE	30-32	☒	L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS	91-102
☒	G	CONTRACT ADMINISTRATION DATA	33-42	☒	M	EVALUATION FACTORS FOR AWARD	103-107
☒	H	SPECIAL CONTRACT REQUIREMENTS	43-50				

OFFER (Must be fully completed by offeror)

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within <u>120</u> calendar days (60 calendar days unless a different period is inserted by the offeror) from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.					
13. DISCOUNT FOR PROMPT PAYMENT (See Section I, Clause No. 52.232.8)		10 CALENDAR DAYS (%)	20 CALENDAR DAYS (%)	30 CALENDAR DAYS (%)	CALENDAR DAYS (%)
14. ACKNOWLEDGEMENT OF AMENDMENTS (The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):		AMENDMENT NO.	DATE	AMENDMENT NO.	DATE
15A. NAME AND ADDRESS OF OFFEROR		CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER (Type or print)	
15B. TELEPHONE NUMBER AREA CODE NUMBER EXTENSION		15C. CHECK IF REMITTANCE ADDRESS ☐ IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.		17. SIGNATURE	18. OFFER DATE

AWARD (To be completed by government)					
19. ACCEPTED AS TO ITEMS NUMBERED		20. AMOUNT		21. ACCOUNTING AND APPROPRIATION	
22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION UNDER THE UNITED STATES CODE AT: ☐ 10 U.S.C. 3204 (a) () ☐ 41 U.S.C. 3304 (a) ()				23. SUBMIT INVOICES TO ADDRESS SHOWN IN (4 copies unless otherwise specified)	
24. ADMINISTERED BY (If other than Item 7) CODE				25. PAYMENT WILL BE MADE BY CODE	
26. NAME OF CONTRACTING OFFICER (Type or print) NICHOLAS C. BISHAR				27. UNITED STATES OF AMERICA (Signature of Contracting Officer)	
				28. AWARD DATE	

NAME OF OFFEROR OR CONTRACTOR

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1	This is a combined synopsis/solicitation for commercial services prepared in accordance with the format set forth at Revolutionary Federal Acquisition Regulation (FAR) Overhaul (RFO) FAR 12.202(b)(1) (Apr. 20, 2026) [adopted via Department of Health and Human Services (HHS) FAR Class Deviation (CD) No. 2025-09, Amendment 1 (Nov. 3, 2025)]. This announcement constitutes the only solicitation. Offers are being requested, and a separate written solicitation will not be issued. This acquisition is exclusively set aside for Service-Disabled Veteran-Owned Small Business (SDVOSB) concerns in accordance with RFO FAR 19.106-2 (Feb. 20, 2026) [adopted via HHS FAR CD No. 2026-01, Amendment 2 (Apr. 24, 2026)]. Status as an SDVOSB concern is determined by the Small Business Association (SBA) in accordance with 13 Code of Federal Regulations (CFR) part 128. Solicitation number 75F40126R00009 is issued as a request for proposal (RFP) for Contractor-Hosted Fully Integrated Records Facility (FIRF) services. The Government anticipates awarding a single Indefinite Delivery, Indefinite Quantity (IDIQ) contract that will allow for Time-and-Materials (T&M), Labor-Hour (LH), and Firm-Fixed Price (FFP) type Task Orders, or a combination thereof. This anticipated IDIQ will contain a five (5) year ordering period, which will be from the date of award through five (5) years unless extended as applicable. Period of Performance: 10/30/2026 to 10/29/2031 Contractor-Hosted Fully Integrated Records Facility (FIRF) services. IDIQ ceiling: \$50,000,000.00. IDIQ guaranteed minimum: \$10,000.00.				

Part I – The Schedule

Section A, Solicitation/contract form

A.1 NOTICE OF COMBINED SYNOPSIS/SOLICITATION FOR COMMERCIAL SERVICES

This is a combined synopsis/solicitation for commercial services prepared in accordance with the format set forth at Revolutionary Federal Acquisition Regulation (FAR) Overhaul (RFO) FAR 12.202(b)(1) (Apr. 20, 2026) [adopted via Department of Health and Human Services (HHS) FAR Class Deviation (CD) No. 2025-09, Amendment 1 (Nov. 3, 2025)]. This announcement constitutes the only solicitation. Offers are being requested, and a separate written solicitation will not be issued. Solicitation number 75F40126R00009 is issued as a request for proposal (RFP) for Contractor-Hosted Fully Integrated Records Facility (FIRF) services. This is a request for proposal (RFP) for commercial services in accordance with the procedures of RFO FAR Part 12 – Acquisition of Commercial Products and Commercial Services, in conjunction with the procedures of RFO FAR Part 15 – Contracting by Negotiation. See RFO FAR 12.201-2 (Apr. 20, 2026) [adopted via HHS FAR CD No. 2025-09, Amendment 1 (Nov. 3, 2025)].

A.2 NOTICE OF NAICS/SET-ASIDE

This acquisition is a set-aside for Service-Disabled Veteran-Owned Small Business (SDVOSB) concerns eligible under the SDVOSB Program in accordance with RFO FAR 19.106-2 (Feb. 20, 2026) [adopted via HHS FAR CD No. 2026-01, Amendment 2 (Apr. 24, 2026)]. The associated North American Industry Classification System (NAICS) code is 541611- Administrative Management and General Management Consulting Services. The associated small business size standard is \$24.5 million.

Pursuant to RFO FAR clause 52.219-27, Notice of Set-Aside for, or Sole-Source Award to, Service-Disabled Veteran-Owned Small Business (SDVOSB) Concerns Eligible Under the SDVOSB Program (Deviation Date) [HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 19.106-4(a) (Feb. 20, 2026), RFO FAR 52 (July 1, 2026)], Offers are solicited only from concerns designated in the System for Award Management (SAM) as SDVOSB concerns certified by the Small Business Administration (SBA) in accordance with 13 Code of Federal Regulations (CFR) part 128. Offers received from concerns that are not SDVOSB concerns certified by SBA will not be considered. Any award resulting from this solicitation will be made only to a concern designated in SAM as an SDVOSB certified by SBA.

A.3 NOTICE OF FAC

This solicitation document incorporates FAR provisions and clauses in effect through Federal Acquisition Circular (FAC) 2026-01, effective March 13, 2026. This solicitation incorporates provisions and clauses by reference. The full text of provisions and clauses may be accessed electronically at <https://www.acquisition.gov/far/part-52> and at <https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>.

The Department of Health and Human Services (HHS) Acquisition Regulation (HHSAR) provisions and clauses referenced in this solicitation can be found on the following websites:

- HHSAR (effective February 2, 2022): <https://www.acquisition.gov/hhsar/part-352-solicitation-provisions-and-contract-clauses>
- HHSAR Class Deviations: <https://www.hhs.gov/grants-contracts/contracts/contract-policies-regulations/index.html>
- RFO HHSAR Part 352: <https://www.hhs.gov/grants-contracts/contracts/contract-policies-regulations/hhsar-overhaul/rfo-part-352-solicitation-provisions-contract-clauses/index.html>

Section B. Supplies or services and prices/costs

B.1 OVERVIEW OF PRICING SCHEDULE

Offerors shall propose labor categories and labor rates as a completed version of **Attachment C: IDIQ Pricing Worksheet**, to be included in the “Volume 2 – Business/Price Proposal” submission (see **Section L, Instructions, conditions, and notices to offerors or respondents**).

The Contractor’s pricing schedules for labor categories shall contain fully burdened hourly rates. The fully burdened hourly rates for each labor category shall include wages, indirect costs, fringe benefits, overhead, general and administrative, and profit. Hourly rates shall apply to services at both Government and non-Government sites.

By mutual agreement of the parties, additional labor categories may be added to this IDIQ contract to support the tasks of this contract.

B.2 PRICING TERMS

The Contractor shall comply with paragraph (i), *Payment*, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)], regarding the firm-fixed prices for individual Task Orders.

The Contractor shall comply with paragraph (i), *Payments*, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date), Alternate I (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)], regarding the ceiling prices for individual Time-and-Materials (T&M) or Labor-Hour (LH) Task Orders.

B.3 TYPE OF CONTRACT

The Government anticipates awarding a single Indefinite Delivery, Indefinite Quantity (IDIQ) contract that will allow for Time-and-Materials (T&M), Labor-Hour (LH), and Firm-Fixed Price (FFP) type Task Orders, or a combination thereof. This anticipated IDIQ will contain a five (5) year ordering period, which will be from the date of award through five (5) years unless extended as applicable.

B.4 MINIMUM AND MAXIMUM CONTRACT VALUE

(a) The guaranteed minimum for this IDIQ contract is \$10,000.00. It is anticipated that the \$10,000.00 guaranteed minimum will be obligated at time of IDIQ contract award.

(b) The maximum ceiling for this IDIQ contract is \$50,000,000.00.

Section C, Description/specifications/requirements

U.S. FOOD & DRUG ADMINISTRATION (FDA) CONTRACTOR-HOSTED FULLY INTEGRATED RECORDS FACILITY (FIRF) INDEFINITE DELIVERY-INDEFINITE QUANTITY (IDIQ) STATEMENT OF WORK (SOW)

C.1 INTRODUCTION

The mission of the U.S. Food and Drug Administration (FDA) is to protect the health of the American public. For more than one hundred years, FDA has been the international leader ensuring safe food, cosmetics, human drugs, biologics, veterinary products, medical and radiological devices, and tobacco products. As part of its mission, the FDA receives documents from a variety of public and private entities, including regulated industry. Throughout FDA's history, document control and records management has played a vital role in the Agency's regulation process and, ultimately, in the mission to protect public health. This allows FDA to comply with federally mandated document control and record keeping requirements, while maintaining a high level of accountability to the citizens of the United States. To ensure proper organization and management of documents and records materials, the FDA complies with regulations set forth in the Federal Records Act per United States Code (U.S.C.), Title 44, Chapters 29 thru 33; Title 36 Code of Federal Regulations (CFR), Chapter 12; and National Archives and Records Administration (NARA) guidance.

C.2 BACKGROUND

Document control and records management practices are exercised throughout the FDA. This contract encompasses processing documents and records material related to scientific advancement and public health issues at the Contractor-Hosted Fully Integrated Records Facility (FIRF). Due to business strategic initiatives for managing documents and records material, FDA has an ongoing need for flexible accommodations/infrastructure for processing documents and records material.

The FDA regulatory mission supports many laws and Federal regulations that give FDA its mandate. This includes, but is not limited to, Federal Food, Drug and Cosmetic Act, Food and Drug Administration Amendments (FDAAA), Food and Drug Administration Safety and Innovation Act (FDASIA), and other relevant statutes, as follows: Prescription Drug User Fee Act (PDUFA), Medical Device User Fee Act (MDUFA), Clinical Laboratory Improvement Amendments (CLIA), Medical Device Amendments, Safe Medical Devices Act, Electronic Product Radiation Control Provisions of the Food Drug and Cosmetics Act (formerly the Radiation Control for Health and Safety Act), Biosimilar User Fee Act (BsUFA), Animal Drug User Fee Act (ADUFA), Animal Generic Drug User Fee Act (AGDUFA), Mammography Quality Standards Act (MQSA), Export Reform and Enhancement Act (EREA), Freedom of Information Act (FOIA), Family Smoking Prevention and Tobacco Control Act (FSPTCA), and Food Safety Modernization Act (FSMA).

The FDA is required by law to regulate the cosmetic, pharmaceutical, food, tobacco, animal drug, and medical device industries. Regulatory submissions are applications submitted by industry that describe the content and use of products and require FDA review.

Regulatory submissions vary across Centers but typically fall in one of the following categories: pre-market or post-market. Pre-market submissions include pre-application materials, investigational applications, new product applications, and license applications. Post-market submissions include supplemental applications to marketed products, registration and listing information, export applications and certificates, allegations of regulatory misconduct, recalls, Freedom of Information Act (FOIA) requests, and promotional materials. For more detail regarding specific regulatory submissions and associated forms, see the following hyperlink:
<https://www.fda.gov/about-fda/reports-manuals-forms/forms>.

C.2.1. DOCUMENT/RECORDS MANAGEMENT TECHNICAL ENVIRONMENT

FDA's Contractor-Hosted Fully Integrated Records Facility (FIRF) ensures timely receipt, processing, temporary

storage, and distribution of applications to the FDA reviewer community. Currently, there is an off-site Contractor-hosted FIRF. This FIRF provides full life cycle records operations and support.

FDA desires to further the cost savings to the Agency and address space constraints through the consolidation of like functions performed by contractors supporting the off-site Contractor-hosted FIRF. This type of work environment provides FDA with increased flexibility regarding managing space constraints to achieve cost savings.

The FDA FIRF processed over 3,529,079 paper and electronic application submissions in Fiscal Year (FY) 2025. Each application submission may have multiple record keeping transactions (e.g., document preparation, imaging, login, hold, amendments, log out, and issuance of correspondence for purposes of gathering additional information to support or close the review). Therefore, the number of transactions will be substantially greater than the number of unique application submissions.

The FDA receives materials from sources internal and external to the agency, which includes, but is not limited to, paper and electronic. Materials include e-mails, documents, letters, memoranda, completed forms, URLs, graphics, photographs, audio and video recordings, diskettes, DVDs, CDs, microfiche, microfilm, USB drives, and hard drives. In addition, FDA receives physical artifacts such as labels, bottles, syringes, laboratory samples, feed bags, and boxes.

In addition, some Centers accept electronic copies (eCopy submissions). An electronic copy is an exact duplicate of a paper submission. It may be received on a CD, DVD, USB drive, or external hard drive accompanied by a copy of the signed cover letter. It may also be received electronically through the electronic submissions gateway or CDRH Portal with no accompanying cover letter. CDRH also accepts eSTAR submissions. Certain submission types are required in eSTAR format instead of eCopy format. When eSTAR is required, the CDRH Portal or electronic submissions gateway is also required, with few exceptions.

C.2.2. 21ST CENTURY ELECTRONIC BASED RECORDS INFORMATION MANAGEMENT (RIM) ENVIRONMENT

The FDA strives towards a streamlined 21st Century electronic Records Information Management (RIM) Lifecycle environment that preserves the integrity of public records while creating cost efficiencies that allow the Agency to focus on advancing in scientific and public health efforts. FDA recognizes that electronic submissions have many advantages over paper submissions. By storing electronic submissions in Electronic Document Rooms (EDRs), they are always readily accessible to reviewers. The FDA's goal is to be 100% electronic.

Currently, FDA receives electronic submissions in structured and unstructured formats for regulatory submissions. Cosmetic, pharmaceutical, food, and medical device or electronic product regulatory submissions, which are applications submitted by industry, provide required information to the FDA to comply with the regulations for regulated products. Regulatory submissions vary across Centers but typically fall into one of the following categories: pre-market or post-market.

C.3 PURPOSE

The purpose of this Indefinite Delivery-Indefinite Quantity (IDIQ) contract is to obtain Contractor services related to several document control and records-related activities throughout FDA, to be performed at the Contractor-Hosted FIRF. This includes receiving, processing, inventorying, scanning services, disposing of documents and records materials, cataloguing, storage of documents, materials, redaction, data entry, helping firms with submitting information electronically, running reports/queries, correcting, and entering data into electronic systems and emailing correspondence to firms.

C.4 OBJECTIVES

The Contractor shall provide services and solutions for the processing of documents, records material and information, such as:

1. Standardizing records management processes;
2. Promoting transparency and accountability by better documenting Agency actions and decisions;

3. Moving to near 100% electronic environment for new premarket and postmarket submissions;
4. Implementing and promoting operational efficiencies; and
5. Implementing and promoting cost efficiencies.

C.5 SCOPE

Independently and not as an agent of the Government, the Contractor shall furnish the necessary personnel, materials, services, and facilities to do all things necessary for or incidental to the performance of the work for Contractor-hosted offsite document control services. This includes receiving, processing, inventorying, scanning services, disposing of documents and records materials, cataloguing, storage of documents and materials, redaction, data entry, helping firms with submitting information electronically, running reports/queries, correcting, and entering data into electronic systems and emailing correspondence to firms. The Contractor shall be responsible for complete management of the FIRF in which services are provided.

C.6 TASKS AREAS

The FDA Off-Site regulatory document and records control and electronic submissions handling processes are divided into the following major task areas:

- Task Area 1: Program and Task Order Management Support;
- Task Area 2: Document Processing, Handling, Correspondence, and Delivery;
- Task Area 3: Document Scanning, Photocopying, Conversion, and Pre-market Services;
- Task Area 4: Document Data Entry Services, Data Analysis, Tracking Services, and Stakeholder Support;
- Task Area 5: Tracking and Temporary Storage of Government Records; and
- Task Area 6: Transition Work Activities

C.6.1. TASK AREA 1: PROGRAM AND TASK ORDER MANAGEMENT SUPPORT

The Contractor shall provide the program management services necessary to plan, structure, coordinate, schedule, manage, communicate, report, and steward all Task Orders (TOs) and activities throughout the IDIQ contract's period of performance. The Contractor shall provide both Contract-level Program Management task support and TO-level project management task support to establish control, management, monitoring, and notification mechanisms, and shall work with the Government Contracting Officer (CO), Contracting Officer's Representative (COR), Task Order Project Managers (TOPMs), and Subject Matter Experts (SMEs) to ensure that tasks stay on track and important milestones are met.

C.6.2. TASK AREA 2: DOCUMENT PROCESSING, HANDLING, CORRESPONDENCE, AND DELIVERY

Documents and records material shall be received at the FIRF. The Contractor shall receive U.S. Mail and deliveries via commercial, private couriers, and will also receive electronic documents (e.g., via online portals, email, or other mechanisms that require processing). Specific mail room processes will be identified in the individual TOs. The Contractor shall be required to staff the mail room, monitor electronic document systems, including emails, sort documents received, prioritize, triage, scan, bar-code/track, and distribute both hard copy and electronic regulatory submissions to the FDA community, or coordinate with U.S. mail couriers and others. The Contractor shall be responsible for tracking all documents to and from the FIRF and the FDA White Oak campus.

As tasked, the Contractor shall process required and voluntary eCopies of submissions provided to FDA on an electronic media (e.g., CD) into the official repository. The Contractor shall perform at least 95% same-day processing for each submission type.

The FDA creates and receives a variety of non-regulatory Federal records. This includes, but is not limited to, program records, office administration records, and dockets. The Contractor shall provide user support services to internal and external stakeholders. Some examples of user support services are responding to inquiries regarding the status of documents being processed, assisting firms with entering data into an electronic system to comply with regulatory requirements, and searching for records to respond to Freedom of Information Act (FOIA) requests.

In addition, the Contractor shall perform tasks related to, but not limited to, document and records information processing. As tasked, the Contractor shall provide courier service to multiple FDA facilities each weekday. The Contractor shall be responsible for providing courier services and distributing mail and stored files between off-site and on-site locations and coordinating pick-up and drop-offs as identified in individual TOs. The FDA distributes documents and records materials to FDA employees, managers, and Contractor staff. New incoming regulatory submissions are primarily distributed to the FDA reviewer community. Non-regulatory material may go to the FDA reviewer community, Contractor staff, administrative staff, and program managers, as needed/or instructed. Distribution locations can be modified or changed throughout the review process for various reasons; thus, requiring data entry changes in the applicable tracking system. The Contractor shall also provide expedited delivery services of FDA materials. Expedited delivery is within one (1) to two (2) hours of an order being placed. The Contractor shall deliver records materials after hours, as required. After hours are after normal business hours (8:00 am – 5:00 pm) Monday through Friday, weekends, and holidays. The Contractor shall be responsible for providing back-up couriers/drivers services in the event courier support services are required after hours.

C.6.3. TASK AREA 3: DOCUMENT SCANNING, PHOTOCOPYING, CONVERSION, AND PRE-MARKET SERVICES

The Contractor shall perform off-site scanning services for pre-market and post-market documents (paper, legacy (historical) paper copy and microfiche submissions), which may range from digitizing legacy material to processing new physical documents and records material. The Contractor shall first verify whether the submission is loaded into IMAGE. If the submission has not been loaded into IMAGE, the Contractor shall scan and index the submission and perform a Quality Control (QC) on the images to ensure the quality and accuracy of the scans. Once the submission has been verified in IMAGE, the Contractor shall destroy the documents immediately (unless subject to applicable Federal records policy). Most scanned services will be from paper to electronic images. The Contractor shall also convert material such as film, videos, microfiche, blowbacks, and physical artifacts into digitized images. Requirements for off-site scanning, photocopying, conversion, and pre-market services will vary and will be outlined in the individual TOs.

C.6.4. TASK AREA 4: DOCUMENT DATA ENTRY SERVICES, DATA ANALYSIS, TRACKING SERVICES, AND STAKEHOLDER SUPPORT

The Contractor shall be responsible for using a database system (i.e., a combination of FDA existing systems and the Contractor's system which will be used to determine where a document is located at any given time) to conduct scheduled inventories of documents and records located at the FIRF and to track the real-time file movement (and status of files) between FDA on-site and off-site locations. FDA Document and Records Managers need real-time access to the inventory data which allows FDA to track the location of documents and determine the status of documents (e.g., change status of files from active to inactive). As tasked, the Contractor shall upload inventories of documents and records information into Center-specific tracking systems and databases and provide direct access to their tracking system by Application Programming Interface (API) or some other means to allow for real time data acquisition by FDA. The Contractor's tracking system must meet all requirements listed in the FDA/CDRH Document Control Center (DCC) Tracking System Requirements (**Attachment A: Statement of Work Appendices, Appendix 5: FDA-CDRH Document Control Center (DCC) Tracking System Requirements**).

C.6.5. TASK AREA 5: TRACKING AND TEMPORARY STORAGE OF GOVERNMENT RECORDS

The Contractor shall be responsible for notifying the IDIQ COR, TO COR, Task Order Project Manager (TOPM), and Center's Records Manager when the Records Control Schedules (RCSs) indicate a file is ready for retention and/or disposal. The Contractor shall obtain written authorization from the Center's Records Manager before moving or disposing of files. The FDA classifies retention and disposal schedules by the following record types: administrative, program, or Center-Specific. The Agency regularly analyzes, develops, produces, and updates FDA RCSs for the Agency, as well as for the individual Centers.

C.6.6. TASK AREA 6: TRANSITION WORK ACTIVITIES

Transition activities shall take place to efficiently transition TO requirements from the predecessor Contractor to the successor Contractor, upon the completion of this contract, if necessary. As tasked, the Contractor may be required

to develop transition-in and transition-out plans for individual TOs issued against this IDIQ contract based on individual requirements.

C.6.6.1. TRANSITION-IN

A smooth and orderly transition-in from the predecessor Contractor to the successor Contractor is necessary to ensure minimum disruption to vital FDA business. Transition-In Plans shall include, at a minimum, a description of parallel operations, management plans, personnel on-boarding process tracking, and an updated list of Contractor personnel, with anticipated start dates and responsibilities. The Contractor shall cooperate fully in transition activities. The Contractor shall work with the FDA Help Desk Support during the transition to implement the Help Desk Support Project Plan for any large-scale relocation/movement of equipment. This shall include, but may not be limited to, the relocation/movement of FDA IT computer equipment, such as computer monitors, keyboards, mice, laptop and desktop computers, printers, scanners, or any other peripherals.

C.6.6.2. TRANSITION-OUT

A smooth and orderly transition-out from the predecessor Contractor to the successor Contractor is necessary to ensure minimum disruption to vital FDA business. The Contractor shall be required to submit and execute a Transition-Out Plan to ensure business continuity for the FDA in the event there is a successor Contractor. This shall include, at a minimum, the following:

- Transition-Out Plan and Schedule;
- Scheduling of knowledge walkthrough sessions;
- Providing “shadowing” and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by the Contractor;
- Submitting knowledge transfer documentation, to include current and up-to-date Standard Operating Procedures (SOPs); and
- Providing FDA with current inventory of all Government-owned assets used by the Contractor, along with full support in the reconciliation of this inventory.

To accommodate strategic initiatives for creating cost and operational efficiencies, the FDA anticipates FIRF locations and housed documents may change between various locations during the life of this IDIQ contract. As tasked, the Contractor shall assist with the preparation and movement of documents between current facilities and new or existing sites. The Contractor shall be required to manage documents and other submissions in a timely and secure manner during day-to-day planned activities and facility relocation in accordance with FDA processing guidance and policies.

C.7 FACILITY REQUIREMENTS

C.7.1. INFRASTRUCTURE AND EQUIPMENT REQUIREMENTS

All infrastructure must obtain an Authorization to Operate (ATO) certificate from FDA, which certifies the FIRF and IT equipment that are proposed to process FDA’s documents are compatible with FDA’s physical and logical environments.

All Contractor-provided equipment connected to FDA’s network must be isolated for FDA business exclusively and may not be used to process any non-FDA business. Therefore, the FDA technical environment must be separated from the Contractor’s internal technical environment.

C.7.2. FDA DIRECT DATA CABLE

Upon award of the first TO issued under this IDIQ contract, the Government will be responsible for purchasing, installing, and maintaining a Verizon data cable line that directly connects from the FDA White Oak Campus to the Contractor’s facility, if applicable.

The Contractor shall safely conceal data outlets, and the associated wiring used to transmit data to workstations must be in floor ducts, walls, columns, or below access flooring. The Contractor shall provide outlets, which must include

rings and pull strings to facilitate the installation of the data cable. When cable consists of multiple runs, the Contractor shall provide ladder-type or other acceptable cable trays to prevent Government-provided cable from coming into contact with suspended ceilings or sprinkler piping. Cable trays must form a loop around the perimeter of the Government-demised area such that they are within a 30-foot horizontal distance of any single drop.

C.7.3. OFF-SITE FACILITY MANAGEMENT

The FIRF must comply with Federal Information Security Management Act (FISMA) and supplemental policies for securing document and records material and information.

The Contractor shall comply with all Federal, state, and local laws, codes and ordinances applicable to use and occupancy of Real Property, including, without limitation, laws applicable to the construction, ownership, alteration, maintenance or operation of all buildings, structures, and facilities located thereon, and obtain all necessary permits, licenses and similar items at its own expense. This contract shall be governed by Federal law.

C.7.4. PHYSICAL ACCESS CONTROLS

Entrance into the Contractor-Hosted FIRF must be through controlled entry point(s). Visitors shall be required to sign in and out at the entrance and state the purpose of their visit. A log shall be kept of all such visits. Persons that do not have a legitimate business need related to the facility operation shall not be allowed access to the FIRF.

C.7.5. NETWORK ACCESS CONTROLS

Contractors accessing FDA's Virtual Private Network (VPN) from off-site locations to manage records information must be connected to the FDA network through an FDA authorized secure channel, such as Cisco AnyConnect/Zscaler. All Contractor staff accessing FDA's network from remote locations are subject to FISMA regulations. The FDA reserves the right to inspect the FIRF to verify FISMA compliance. Please note, Contractor staff may not access the FDA network via their personal computers. If a direct connection is required from the FIRF to the FDA network due to bandwidth or security reasons, the Government will provide the Contractor with all necessary specifications for the Contractor to provide proper connectivity.

C.8 KEY PERSONNEL

The Contractor shall provide sufficient personnel possessing the skills, knowledge, training, and security clearances to perform the services required by this IDIQ. The Government requires a balanced team of personnel to ensure operational (budgetary/financial) and technical aspects of the IDIQ are successful.

It is critical that the Contractor is committed to maintaining consistency in key personnel and staff assignments for the duration of the FIRF IDIQ contract and Task Orders issued under the IDIQ.

The Contractor shall ensure that personnel maintain generally required professional certifications, accreditations, and proficiency relative to their areas of expertise (as defined in the labor category descriptions and minimum requirements set forth in **Attachment F: Labor Category Descriptions**). The training of Contractor personnel to fulfill these requirements shall be provided at the Contractor's expense. The Contractor shall retain documentation of such records.

C.8.1. HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) 352.237-75 KEY PERSONNEL (DEC 2015)

The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to the contractor voluntarily diverting any of the specified individuals to other programs or contracts the Contractor shall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the contract (including, when applicable, Human Subjects Testing requirements). If the employee of the contractor is terminated for cause or separates from the contractor voluntarily with less than thirty days' notice, the Contractor shall provide the

maximum notice practicable under the circumstances. The Contractor shall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The contract will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

The following individual will be designated as Key Personnel at the IDIQ contract level:

Position	Labor Category	Name of Individual
Program (Contract) Manager	<i>To be determined at time of award</i>	<i>To be determined at time of award</i>

Key Personnel may also be identified within each TO.

C.9 LABOR CATEGORY DESCRIPTIONS AND MINIMUM REQUIREMENTS

See **Attachment F: Labor Category Descriptions** in **Section J, List of attachments**.

C.10 OCCUPATIONAL SAFETY AND HEALTH TERMS AND CONDITIONS

GENERAL OCCUPATIONAL SAFETY AND HEALTH TERMS AND CONDITIONS:

1. The contractor is responsible for ensuring contractor personnel comply with applicable OSHA requirements, report unsafe conditions or activities to the Contracting Officer's Representative (COR), and avoid actions and conditions that may result in an accident.
2. The contractor shall submit to the COR a site-specific safety and accident prevention plan and OSHA 300A reports from the past three calendar years.
3. The contractor shall report all workplace incidents, accidents, injuries, and near-misses that occur within the scope of the acquisition (whether OSHA-recordable or not) to the COR by email as soon as possible, but no more than 24-hours after discovery of the incident, illness or injury, or near-miss.
4. The contractor shall provide an investigation report at no cost to the Government for all workplace incidents, accidents, injuries, and near-misses that occur within the scope of the acquisition (whether OSHA-recordable or not) to the COR by email as soon as possible, but no more than 24-hours after the conclusion of the investigation of the incident, illness or injury, or near-miss.
5. The contractor shall report all activities or conditions that pose imminent danger or harm to persons, animals, or Government property immediately upon discovery to FDA Security or directly to local emergency services, as appropriate. In addition, the contractor shall report the incident to the COR immediately thereafter.
6. The contractor shall be responsible for any and all costs, expenses, and other obligations paid or incurred, due to the contractor's noncompliance with federal, state, and/or local laws or ordinances.
7. As applicable, the contractor shall provide personal protective equipment (e.g., hard hats, safety glasses, work gloves) for anticipated hazards and ensure that contractor personnel wear the prescribed safety and health equipment within the work area, as prescribed by 29 CFR part 1910, Subpart I. The contractor shall provide instructions to personnel on the proper wear, maintenance, and limitations of the personal protective equipment prior to commencement of any work under the acquisition.
8. Prior to bringing any hazardous material to an FDA facility, the contractor shall provide the COR copies of any Safety Data Sheets (SDS) to obtain advance, written authorization.
 - a) Unless otherwise specified in the acquisition, the contractor is responsible for removing any hazardous material, or any material with an SDS, that the contractor brought with them for use at an FDA facility before or during performance of the acquisition.

C.11 PROCUREMENTS REQUIRING INFORMATION SECURITY AND/OR PHYSICAL ACCESS SECURITY

1. Baseline Security Requirements

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

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

ii. **Operate a Federal System Containing Information:** A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the FDA mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

b. **Safeguarding Information and Information Systems.** All government information and information systems must be protected in accordance with FDA policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:

i. Protect the:

- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
- **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
- **Availability**, which means ensuring timely and reliable access to and use of information.

ii. Categorize all information owned and/or collected/managed on behalf of FDA and information systems that store, process, and/or transmit FDA information in accordance with FIPS 199 and National Institute of Standards and Technology ([NIST\) Special Publication \(SP\) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories](#). Based on information provided by the System/Data Owner, ISSO, privacy representative, or other POC, the impact level for each Security Objective (Confidentiality, Integrity, and Availability) and the Overall Impact Level, which is the highest watermark of the three factors of the information or information system are the following:

- **Confidentiality:** ☐ Low ☐ Moderate ☒ High
- **Integrity:** ☐ Low ☐ Moderate ☒ High
- **Availability:** ☐ Low ☒ Moderate ☐ High
- **Overall Impact Level:** ☐ Low ☐ Moderate ☒ High

iii. Based on the agreed-upon level of impact, implement the necessary safeguards to protect all information systems and information collected and/or managed on behalf of FDA regardless of location or purpose.

iv. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s). This includes notifying the FDA Cybersecurity and Infrastructure Operations Coordination Center (CIOCC) within one (1) hour of discovery/detection in the event of a cybersecurity or privacy incident.

v. Adopt and implement all applicable policies, procedures, controls, and standards required by the FDA Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the FDA Information Security Program security requirements, outlined in the

Contractor-Hosted Fully Integrated Records Facility (FIRF) IDIQ Recompete
Request for Proposal (RFP) No. 75F40126R00009

FDA Information Security and Privacy Protection (IS2P) policy, by contacting the CO/COR or emailing your ISSO.

c. **Privacy Act.** Comply with the Privacy Act requirements (when applicable), and tailor FAR and HHSAR clauses as needed.

d. **Privacy Compliance.** Comply with the E-Government Act of 2002, NIST SP 800-53, and applicable FDA privacy policies and complete all the requirements below:

i. Per the Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII), is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: Social Security number, date and place of birth, mother's maiden name, biometric records, etc.

ii. Based on information provided by the ISSO, System/Data Owner, or other security or privacy representative, it has been determined that this solicitation/ contract involves:

☐ No PII ☒ PII

iii. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed.

- If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information after completion of the PTA and in accordance with HHS and FDA policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. The PTA/PIA must be completed and approved prior to active use and/or collection or processing of PII and is a prerequisite to agency issuance of an authorization to operate (ATO).
- The Contractor must support the agency in reviewing the PIA at least every **three years** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

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

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 FDA 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*.

f. **Protection of Sensitive Information.** For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

g. **Government Furnished Equipment (GFE) for Foreign Travel.** FDA personnel are prohibited from taking GFE when participating in personal, unofficial travel to foreign countries. FDA personnel are strictly prohibited from teleworking using GFE in foreign countries.

h. **Confidentiality and Nondisclosure of Information.** Any information provided to the contractor (and/or any subcontractor) by FDA or collected by the contractor on behalf of FDA must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any FDA records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

The confidentiality, integrity, and availability of such information must be protected in accordance with HHS and FDA policies. Unauthorized disclosure of information will be subject to the HHS and FDA 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).

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

j. **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.

k. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.

l. **Contract Documentation.** The Contractor must use provided templates, policies, forms, and other agency documents to comply with contract deliverables as appropriate.

m. **Standard for Encryption.** The Contractor (and/or any subcontractor) must:

- i. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
- ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e.,

servers, storage devices, mobile devices, backup media, etc.) with an encryption solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.

iii. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and FDA-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificates from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR.

v. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys <http://csrc.nist.gov/publications/>. Encryption keys must be provided to the COR upon request and at the conclusion of the contract.

n. **Contractor Non-Disclosure Agreement (NDA).** Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the FDA non-disclosure agreement (see **Attachment H: Commitment to Protect Non-Public Information (NPI) Employee Agreement Form FDA 3398**), as applicable. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

2. Training Requirements

a. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract must complete the applicable FDA information security awareness, privacy, and records management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees must complete FDA information security awareness, privacy, and records management training at least **annually**, during the life of this contract. All provided training must be compliant with HHS training policies.

b. **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training **annually** commensurate with their role and responsibilities in accordance with HHS and FDA policy.

c. **Training Records.** The Contractor (and/or any subcontractor) must maintain training records for all its employees working under this contract in accordance with HHS and FDA policy. A copy of the training records must be provided to the CO and/or COR within **30 days** after contract award and **annually** thereafter or upon request.

3. Rules of Behavior

a. The Contractor (and/or any subcontractor) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*, *HHS Rules of Behavior for Privileged Users*, and FDA policies and standards.

b. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Agency data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least **annually** thereafter, which may be done as part of annual FDA Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

4. Incident Response

a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/FDA CIOCC /Incident Response Team teams **within 24 hours**, whether the response is positive or negative.

FISMA defines an incident as “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.” In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is “an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies” and a privacy breach is “the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.” For additional information on the HHS breach response process, please see the FDA IS2P Appendix F: Incident Response and the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*.

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

i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.

ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so, instructed by the Contracting Officer or representative, the Contractor must send FDA approved notifications to affected individuals as directed by FDA’s SOP.

iii. Report all suspected and confirmed information security and privacy incidents and breaches to the FDA CIOCC, COR, CO, FDA SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable FDA and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:

- Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
- Not include any sensitive information in the subject or body of any reporting e-mail; and
- Encrypt sensitive information in attachments to email, media, etc.

iv. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and HHS and FDA breach response policies when handling PII breaches.

v. Provide full access and cooperate on all activities as determined by the Government to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. This may involve disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls. This may also involve physical access to contractor facilities during a breach/incident investigation on demand.

5. Position Sensitivity Designations

All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract (e.g. tier 1, 2, or 4): Tier 2/Sensitive Moderate Risk.

6. Homeland Security Presidential Directive (HSPD)-12

The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; OMB M-05-24; OMB M-19-17; FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; HHS HSPD-12 policy; and *Executive Order 13467, Part 1 §1.2*.

7. Roster

The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO per the COR or CO's direction. Any revisions to the roster as a result of staffing changes must be submitted within a timeline as directed by the COR and/or CO. The COR will notify the Contractor of the appropriate level of investigation required for each staff member.

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

8. Contract Initiation and Expiration

a. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the Contractor must follow the FDA EPLC framework and methodology in accordance with the FDA EPLC Project documentation, located here: <http://sharepoint.fda.gov/orgs/DelMgmtSupport/IntakeProc/EPLCv2/SitePages/v2/EPLCHome.aspx> and in accordance with the HHS Contract Closeout Guide (2012).

b. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

c. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation in accordance with SMGs published by FDA's Office of Acquisitions and Grant Services (OAGS) to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

d. **Notification.** The Contractor (and/or any subcontractor) must notify the CO and/or COR and system ISSO as soon as it is known that a contract employee will stop working under this contract.

e. **Contractor Responsibilities upon Physical Completion of the Contract.** The Contractor (and/or any subcontractors) must return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and FDA policies.

f. The Contractor (and/or any subcontractor) must perform and document the actions identified in the FDA eDepart system, <http://inside.fda.gov:9003/EmployeeResources/NewEmployee/eDepartDepartureSystem/default.htm>, as soon as it is known that a Contractor employee will terminate work under this contract. The Contractor (and/or any subcontractor) shall coordinate with the COR via email, copying the Contract Specialist, to ensure that the appropriate person performs and documents the actions identified in the FDA eDepart system. All documentation must be available to the CO and/or COR upon request.

9. Records Management and Retention

- a. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *HHS Policy for Records Management* and HHS and FDA policies and must not dispose of any records unless authorized by HHS and FDA.
- b. In the event that a Contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS and FDA policies.

10. High Value Asset (HVA)

If a system is identified as HVA, the Contractor must comply with the FDA IS2P Appendix AB: High Value Asset (HVA) Program, the HHS Policy for the High Value Asset (HVA) Program, and the DHS HVA Control Overlay in addition to the above requirements.

C.12 PROCUREMENTS INVOLVING GOVERNMENT INFORMATION PROCESSED ON GOVERNMENT-OWNED/CONTRACTOR-OPERATED (GOCO) OR CONTRACTOR-OWNED/CONTRACTOR-OPERATED (COCO) SYSTEMS

1. Security Requirements for GOCO and COCO Resources

- a. **Federal Policies.** The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS and FDA policies that include, but are not limited to, the *HHS Information Security and Privacy Protection (IS2P)* policy; *FDA Information Security and Privacy Protection (IS2P)* policy; *Federal Information Security Modernization Act (FISMA) of 2014*, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, Departmental, and Agency 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 (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s): **Within 30 days**. The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ FDA IS2P* 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).

FDA acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

- i. **A&A Package Deliverables** - The Contractor (and/or any subcontractor) must provide an A&A package within a timeline directed by the COR, per the FDA Enterprise Performance Lifecycle (EPLC) process, to the CO and/or COR. The following A&A deliverables are required to complete the A&A package:

1. **System Security Plan (SSP)** - due a week prior to the start of the annual security assessment. The SSP must comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and FDA policies and other guidance. The SSP must be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP must provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor must review and update the SSP at least **annually** thereafter and if requested, provide a copy of the updated SSP.
2. **Security Assessment Plan/Report (SAP/SAR)** - due before the system is made available to standard users. The security assessment must be conducted by FDA's team of security assessors, unless otherwise noted and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and FDA policies. The assessor will document the assessment results in the SAR.

Thereafter, the Contractor, in coordination with FDA, must assist in the assessment of the security controls and update the SAR at least **annually**. A copy of the updated SAR should be provided if requested.

3. **Independent Assessment** - The Contractor (and/or subcontractor) must have an independent third party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all "high" deficiencies and enter all other deficiencies that require mitigation by Contractor before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Action and Milestones (POA&M).
4. **POA&M** - as part of the SAR All high-risk weaknesses must be mitigated within 30 calendar days moderate weaknesses must be mitigated within 60 calendar days and low weaknesses must be mitigated within 180 calendar days from the date the weaknesses are formally identified and documented. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defects in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones, FDA POA&M Management Guide, and FDA IS2P policies. Depending on the severity of the risks, FDA may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly**.
5. **Contingency Plan and Contingency Plan Test** - due during the annual security assessment. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be

consistent with HHS and FDA policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, must test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor must update and test the Contingency Plan at least **annually**.

6. **E-Authentication Questionnaire** - The Contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B.

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E-Auth (when required) in accordance with *HHS Guidance for Selection of e-Authentication Assurance Levels* and any other applicable HHS and FDA policies.

- ii. **Information Security Continuous Monitoring.** Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, must meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, and HHS and FDA IS2Ps.
- iii. **Annual Assessment/Penetration (Pen) Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the FDA. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date in the deliverable table.
- iv. **Asset Management** – Using FDA-approved Security Content Automation Protocol (SCAP)-compliant automated tools for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing FDA-owned information/data. It is anticipated that this inventory information will be required to be produced at least annually to facilitate management/oversight efforts. IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools in accordance with the *HHS Policy for Information Technology Asset Management (ITAM)* and any other applicable HHS and FDA policies.
- v. **Configuration Management** - Use FDA-approved SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS/FDA upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.
- vi. **Vulnerability Management** - Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with the *FDA Information Security and Privacy Protection (IS2P)* policy and *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for

vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least monthly.

- vii. **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and FDA patch management policy timeframes.
 - viii. **Secure Coding** - Follow the *HHS Policy for Software Development Secure Coding Practices* and secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.
 - ix. **Boundary Protection** - The Contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).
- c. **Government Access for Security Assessment.** In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) must afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS or FDA, including but are not limited to:
- i. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.
- The Government includes but is not limited to the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.
- ii. 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.
- 1. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be

precluded from having access to the sought information if sought information is commingled with other information.

2. Cooperate with inspections, audits, investigations, and reviews.
- d. **End of Life Compliance.** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO if it impacts enterprise-wide systems and services, or by the FDA CISO if it impacts only the FDA). 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* and *FDA End-of-Life Operating Systems, Software, and Applications Policy*.
- e. **Desktops, Laptops, and Other Computing Devices Required for Use by the Contractor.** The Contractor (and/or any subcontractor) must ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of FDA are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:
 - i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FDA encryption standard and current FIPS 140 validation certificate from the NIST CMVP.
 - ii. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), FDA Configuration Baselines, FDA Minimum Security Configuration Standards, and HHS Minimum Security Configuration Standards;
 - iii. Maintain the latest operating system patch release and anti-virus software definitions, per FDA patch management policy;
 - iv. 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
 - v. Automate configuration settings and configuration management in accordance with HHS and FDA security policies, including but not limited to:
 1. Configuring its systems to allow for periodic Federal, HHS, and FDA vulnerability and security configuration assessment scanning; and
 2. Using FDA-approved Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.
- f. **Rights to Data.** All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the Contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.
- g. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements.** The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:
 - i. Develop rules for suppliers' development methods, techniques, or practices;
 - ii. Use of secondary market components;
 - iii. Prohibit counterfeit products;
 - iv. Dispose and/or retain elements such as components, data, or intellectual property securely;
 - v. Ensure adequate supply of components;

- vi. 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;
- vii. 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;
- viii. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
- ix. 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
- x. Prohibit the use of covered telecommunications and video surveillance equipment or services.

C.13 CONTRACTS INVOLVING CLOUD SERVICES

1. HHS FedRAMP Privacy and Security Requirements

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

a. **FedRAMP Compliant ATO.** Comply with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO prior to production implementation

i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *FDA Information Security and Privacy Protection (IS2P) Policy*, *HHS Information Security and Privacy Protection (IS2P) policy* 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 must also implement a set of additional controls identified by the agency when applicable.

ii. A security control assessment must be conducted by a FedRAMP third party assessment organization (3PAO) for the initial ATO and **annually** thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

b. **Data Jurisdiction.** The contractor must store all information within the security authorization boundary, including data at rest, data backups, or other copies within the Continental United States (CONUS).

c. **Service Level Agreements.** The Contractor must abide by the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with FDA to develop and maintain an SLA.

d. **Interconnection Agreements/Memorandum of Agreements.** *Add when applicable* The Contractor must establish and maintain Interconnection Agreements and or Memorandum of Agreements/Understanding in accordance with HHS and FDA policies.

2. Protection of Information in a Cloud Environment

a. If contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they must protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS and FDA policies <https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/index.html>.

b. FDA retains unrestricted rights to federal data handled under this contract. Specifically, FDA retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of FDA and hosted on contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to FDA within **one (1) business day** from request date or within the timeframe specified otherwise. In addition, the data must be provided at no additional cost to FDA.

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

d. The contractor must support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:

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.

e. The disposition of all FDA data must be at the written direction of HHS/ FDA. This may include documents returned to HHS/FDA control; destroyed; or held as specified until otherwise directed. Items returned to the Government must be hand carried or sent by certified mail to the COR.

3. Assessment and Authorization (A&A) Process

a. The Contractor (and/or any subcontractor) must comply with HHS, FDA, and FedRAMP requirements as mandated by federal laws, regulations, and HHS and FDA 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 and FDA security policies.

i. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the FDA authorizing official (AO) prior to implementation of system and/or service being acquired.

ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

iii. For all acquired cloud services, the A&A package must contain the following documentation: See the A&A package deliverables from Section 4 and/or deliverables mentioned in the FedRAMP Standard Contract Language available on the FedRAMP site. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS and FDA policies using FDA templates.

b. DHS, HHS, and FDA reserve the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If DHS/HHS/FDA exercises this right, the Contractor (and/or any subcontractor) must allow DHS/HHS/FDA employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with DHS/HHS/FDA requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other

applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

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

d. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the FDA POA&M Standard, from discovery: (1) critical vulnerabilities no later than **fifteen (15) days** and (2) high within **thirty (30) days** (3) medium within **ninety (60) days** and (4) low vulnerabilities no later than **three hundred and sixty (90) days**. 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 designated timelines.

e. **Revocation of a Cloud Service.** HHS and FDA have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS, FDA, and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or FDA may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

4. Reporting and Continuous Monitoring

a. Following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis:

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 FDA Owner or AO; and

iv. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/FDA's security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

5. Configuration Baseline

a. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *Minimum Security Configuration Standards for FDA Information Technology Systems* and *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 and FDA configuration baseline.

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

6. Incident Reporting

a. The Contractor (and/or any subcontractor) must provide an Incident and Breach Response Plan (IRP) in accordance with HHS, FDAOMB, and US-CERT requirements and obtain approval from FDA. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the FedRAMP Incident Communications.

b. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS and FDA access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection must include, but is not limited to:

i. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/FDA personnel, or agents acting on behalf of HHS/FDA, using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

ii. In the event an incident involving sensitive information occurs, cooperate on all required activities determined by the agency to ensure an effective incident or breach response and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the agency reporting procedures and follow the steps directed by FDA to contain and eradicate the incident, recover from the incident, document the steps taken, and provide a post-incident report that includes at a minimum the following:

- Company and point of contact name;
- Contract information;
- Impact classifications/threat vector;
- Type of information compromised;
- A summary of lessons learned; and
- Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

7. Media Transport

a. The Contractor and its employees must be accountable and document all activities associated with the transport of government information, devices, and media transported outside controlled areas and/or facilities. These include information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards).

b. All information, devices and media must be encrypted with FDA-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities. Storage devices must be approved on the FDA Master Approved Technologies (MAT) list.

8. Boundary Protection: Trusted Internet Connections (TIC)

a. The contractor must ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes that are in compliance with the requirements of the Office of Management and Budget (OMB) Memorandum (M) 19-26: Update to the TIC Initiative, TIC 3.0.

b. The contractor must route all external connections through a TIC.

c. **Non-Repudiation.** The contractor must provide a system that implements encryption with current FIPS 140 validation certificates from the NIST CMVP that provides for origin authentication, data integrity, and signer non-repudiation.

Section D. Packaging and marking

D.1 PACKAGING, MARKING, AND SHIPPING INSTRUCTIONS

Be advised that FDA does not accept documents which contain the use of macros. *When submitting documents via email, DO NOT include .exe, .mso, or any other executable file types that could potentially trigger email security protections (i.e. email blocks, quarantine).* Document submissions required throughout the award period(s) shall not have macro-enabled functionality and any document delivered having that functionality will be deemed delinquent, if not corrected prior to the due date.

All non-electronically submitted deliverables required under this contract shall be packaged, marked and shipped in accordance with the requirements and specifications contained herein this contract. At a minimum, all deliverables shall be marked with the Contract Number and Contractor Name. The Contractor shall guarantee that all required materials shall be delivered in immediate usable and acceptable condition.

Reports not submitted electronically shall be delivered F.O.B. Destination, as set forth in FAR Clause 52.247-35, F.O.B. Destination, Within Consignee's Premises (April 1984), and as specified in the delivery schedule in the TOs.

Unless otherwise specified, deliveries shall be made to the COR on Mondays through Fridays (excluding Federal Holidays and Executive Order), between the hours of 8:00 a.m. and 5:00 p.m., Eastern Time, only. Supplies or services scheduled for delivery on a Federal holiday shall be made the following day.

Section E. Inspection and acceptance

E.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

- <https://www.acquisition.gov/far/part-52>
- <https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>

For Firm-Fixed Price (FFP) Task Orders: The Contractor shall comply with paragraph (b), *Inspection/Acceptance*, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)].

For Time-and-Materials (T&M) or Labor-Hour (LH) Task Orders: The Contractor shall comply with paragraph (b), *Inspection/Acceptance*, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date), Alternate I (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)].

E.2 INSPECTION AND ACCEPTANCE

Satisfactory performance of this contract shall be deemed to occur upon performance of the work and upon delivery and acceptance. The TO Contracting Officer's Representative (COR) will perform inspection and acceptance of materials and services to be provided in each TO. The TO COR is the authorized representative of the TO CO for this section.

If a deliverable is found by the TO COR to be sub-standard, it may require that alterations be made until the deliverable meets the standard expectations at which point it is considered delivered. In some TOs, the deliverable must be 100% accepted by the delivery date. The deliverables and delivery dates will be specified in the TO.

A Quality Assurance Surveillance Plan (QASP) may be included in individual TOs.

Acceptance may be presumed within ten (10) business days of receipt, unless otherwise indicated in writing by the TO CO or TO COR. Inspection and acceptance will be performed at the Place of Performance unless otherwise specified in the individual TOs.

Section F, Deliveries or Performance

F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

- <https://www.acquisition.gov/far/part-52>
- <https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>

FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES:

<u>NUMBER</u>	<u>TITLE</u>	<u>DATE</u>
52.242-15	STOP-WORK ORDER	AUG 1989
52.242-17	GOVERNMENT DELAY OF WORK	APR 1984
52.247-34	F.O.B. DESTINATION	JAN 1991

F.2 PERIOD OF PERFORMANCE

F.2.1 IDIQ ORDERING PERIOD

The anticipated period of performance for this IDIQ contract consists of five (5), 12-month ordering periods, as follows:

- Ordering Period 1: October 30, 2026, through October 29, 2027
- Ordering Period 2: October 30, 2027, through October 29, 2028
- Ordering Period 3: October 30, 2028, through October 29, 2029
- Ordering Period 4: October 30, 2029, through October 29, 2030
- Ordering Period 5: October 30, 2030, through October 29, 2031
- 6-Month Option to Extend Services per FAR clause 52.217-8, Option to Extend Services (Nov 1999): October 30, 2031, through April 29, 2032

The actual period of performance will be determined at time of award.

F.2.2 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for task orders will be specified in individual orders. Individual task orders may not exceed five (5) years and six (6) months (inclusive of option periods). The period of performance end date of a Task Order cannot be later than 5 years after the ordering period end date of the IDIQ.

F.3 PLACE OF PERFORMANCE

The place of performance will be identified in individual TOs, but it is expected to occur primarily at the Contractor-Hosted FIRF facility, with the Contractor providing courier services to multiple FDA facilities. FDA facilities are predominantly located in the Washington, D.C. metropolitan area, with concentrations in the FDA's Maryland locations, including Bethesda, College Park, Laurel, Rockville and Silver Spring.

Specific working arrangements, such as work approved for performance at alternate Contractor locations, will be described in individual TOs.

F.4 HOURS OF OPERATION

Unless otherwise specified in the individual TO, Contractor staff must be available during normal FDA business

hours, from 8:00 am – 5:00 pm Eastern Time (ET), Monday through Friday, except on Government Closures.

The Contractor may be required to deliver documents and records materials outside of normal FDA business hours. If working outside of normal business hours, the Contractor will have the flexibility to use management tools (i.e., swing shifts) to successfully meet individual TO requirements. Any overtime incurred must be approved in advance, in accordance with paragraph (i), *Payments*, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date), Alternate I (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]. Normal FDA business hours are defined as being from 8:00 am – 5:00 pm ET, Monday through Friday, with deliveries on some weekends and holidays.

F.5 GOVERNMENT CLOSURES AND FEDERAL HOLIDAYS

The Contractor may not bill the Government for any hours that Contractor employees did not work due to any Government closure under this contract or any TOs under this contract that include labor-hour or time-and-materials order types. In the event Contractor personnel work during a holiday observed by the Contractor other than those below, no form of holiday or premium compensation will be reimbursed as either a direct or indirect cost. However, this does not preclude reimbursement for authorized overtime work.

Recognized Federal Holidays – Contractor coverage is expected during all Federal workdays. Except for designated around-the-clock or emergency operations and after-hour courier services, Contractor personnel shall not perform on-site services under this contract on the following days that are Federal holidays or on any other day designated as a Federal holiday for the Washington, D.C. metropolitan area. No services or deliveries shall be performed at Federal sites on Federal holidays unless specifically requested by the Contracting Officer. When a holiday falls on a non-workday (Saturday or Sunday) the holiday usually is observed on Monday (if the holiday falls on Sunday) or Friday (if the holiday falls on Saturday).

New Year's Day
Martin Luther King, Jr.'s Birthday
Washington's Birthday
Memorial Day
Juneteenth National Independence Day
Independence Day
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

Inclement Weather and other Government Closures: The Contractor is not required to provide on-site services on days when the Federal Government is closed due to inclement weather, Government closures, or other emergencies. The Contractor is required to follow, as a minimum, other directives issued by the U.S. Office of Personnel Management (OPM) or other such official for late arrivals due to inclement weather (unless otherwise specified in the Contract).

In the event the Federal Government is closed by order of the President of the United States or the U.S. Office of Personnel Management (OPM) for any reason, or the FDA, the Center or the FDA building is closed for administrative or safety reasons, the Contractor shall follow directives issued by OPM or other such official, the COR, and/or the CO concerning reporting to work. In the event of early closings, the Contractor may be approved to leave early at the discretion of the COR, CO, and/or local policy.

If adverse weather conditions develop after the Federal Government has opened for normal business, upon notification of early release from OPM, the COR and/or CO will notify the Contractor of Facility closing and specify the time for a final document pickup.

Additional specific inclement weather plans may be specified at the TO level.

F.6 DELIVERIES

Satisfactory performance of this contract shall be deemed to occur upon performance of the work and acceptance by the Contracting Officer's Representative (COR) or the duly authorized representative.

F.7 DELIVERABLES AND MILESTONES

Specific deliverables and a schedule of deliverables will be identified in each TO.

The Contractor shall submit all preliminary, intermediate, and final deliverables in electronic formats (i.e., Microsoft Office, Adobe, or original source file) to the identified COR. All deliverables that are original source files shall be editable and in the format of the respective product.

Be advised that FDA does not accept documents which contain the use of macros. ***When submitting documents via email, DO NOT include .exe, .mso, or any other executable file types that could potentially trigger email security protections (i.e. email blocks, quarantine).*** Document submissions required throughout the award period(s) shall not have macro-enabled functionality and any document delivered having that functionality will be deemed delinquent, if not corrected prior to the due date.

Section G, Contract administration data

G.1 ORDERING PROCEDURES

The Government will issue individual Task Orders (TOs) under this IDIQ contract in accordance with the ordering procedures set forth at RFO FAR 16.506 (July 1, 2026), Postaward procedures for placement of task and delivery orders [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)].

In accordance with FAR clause 52.216-18(b), Ordering (Aug. 2020), all task orders are subject to the terms and conditions of this IDIQ contract. In the event of conflict between a task order and this IDIQ contract, the IDIQ contract shall control. A task order shall be “issued” for purposes of this contract upon the effective date of the task order.

Ordering services under this contract shall be accomplished by the issuance of written task orders specifying the types of services being ordered. This IDIQ contract is available for use agency-wide (FDA) and only an FDA Contracting Officer is authorized to issue Task Orders against this IDIQ contract.

G.2 PLACEMENT OF ORDERS

A Request for Task Order Proposal (RFTOP) will typically be issued via email to the Contractor’s email address.

Individual Task Orders will clearly describe all services to be performed or supplies to be delivered so the full cost or price for the performance of the work can be established when the order is placed.

In accordance with RFO FAR 16.505(a)(2), Task Orders must be within the scope, issued within the specified ordering period, and be within the maximum value of the IDIQ contract.

In accordance with RFO FAR 16.506(b), all Task Orders placed under this IDIQ contract must contain the following information:

- (1) Date of order.
- (2) Contract number and order number.
- (3) For supplies and services, line-item number, subline item number (if applicable), description, quantity, and unit price or estimated cost and fee (as applicable). The corresponding line-item number and subline item number from the base contract must also be included.
- (4) Delivery or performance schedule.
- (5) Statement of work that clearly specifies all tasks to be performed or property supplies to be delivered under the order. Performance-based acquisition methods must be used to the maximum extent practicable, if the order is for services.
- (6) Place of delivery or performance (including consignee).
- (7) Any packaging, packing, and shipping instructions.
- (8) Accounting and appropriation data.
- (9) Method of payment and payment office, if not specified in the contract (see RFO FAR part 32).
- (10) North American Industry Classification System code (see RFO FAR part 19).

Any work that the Contractor undertakes prior to receiving a fully executed TO that has been signed by the CO (or the Contractor has received prior authorization to proceed from the CO) shall be at the Contractor’s risk.

The general process for individual task orders is as follows:

1. The FDA will prepare a statement of work. The SOW will include, at a minimum, the following elements:
 - a. Description of work in terms of the purpose or objectives of the work to be performed.
 - b. Description of how the work performance is assessed relative to objectives, goals, and outcomes.
 - c. Period and place of performance.
 - d. Reporting requirements and Deliverables.

2. Requests for Task Order Proposals (RFTOP) shall only be issued by the Contracting Officer.
3. The Contractor shall prepare and submit a task proposal addressing all areas of the requirement. The Contractor shall submit the task proposal within the time period specified in the RFTOP and adhere to the ceiling amount established in the contract. No separate payment will be made to the contractor for the cost to prepare, submit and/or negotiate a task order proposal.
4. The Government will evaluate task order proposals for technical acceptability and price reasonableness.

G.3 EMERGENCY ORDERS

In emergency situations or other times when it is not practical to prepare a written work plan prior to the commencement of work, the CO may verbally authorize performance to commence immediately, so long as the work to be performed in the emergency situation is within the scope of this contract. In those instances, a written work plan shall be submitted within ten (10) business days following the authorization to commence work. When work is authorized to commence prior to the submission and negotiation of a work plan, the CO will indicate, at time of authorizing work, a dollar ceiling that may not be exceeded except at the Contractor's own risk.

G.4 PRICING OF ORDERS

Proposals submitted in response to a RFTOP must use labor rates equal to or less than the established IDIQ Ordering Period labor rates listed in the IDIQ Price Schedule based on the performance start date of the TO, and that rate must be used for the duration of the TO performance period; however, if a TO's performance period is longer than twelve (12) months, the Contractor may propose the applicable ordering period rate for that portion of the performance period after the twelve (12) month period. The Contractor may propose lower rates in response to a RFTOP. RFTOPs may include option periods in accordance with FAR clause 52.217-9, Option to Extend the Term of the Contract (Mar 2000).

The Contractor shall comply with paragraph (i), Payment, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)], regarding the firm-fixed prices for individual Task Orders. The total amount specified in FFP DOs/TOs shall be fixed for the TO period of performance and shall not be subject to adjustment; except, as a result of a direct action or inaction by the Government, which delays the Contractor from completing the TO within the time specified in the order.

The Contractor shall comply with paragraph (i), Payments, of RFO FAR clause 52.212-4 Terms and Conditions—Commercial Products and Commercial Services (Deviation Date), Alternate I (Deviation Date) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)], regarding the ceiling prices for individual Time-and-Materials (T&M) or Labor-Hour (LH) Task Orders. LH and T&M TOs will include a ceiling price. If a TO's stated period of performance must be extended as a result of Government delay, the Contractor may request that the most current labor rates be used to price the work effort during the extended period for LH and/or T&M TOs.

The Contractor's pricing schedules for labor categories shall contain fully burdened hourly labor rates, including all wages, indirect costs, fringe benefits, overhead, general and administrative, and profit. Hourly rates apply to services at both Government and non-Government sites. By mutual agreement of the parties, additional labor categories may be added to this IDIQ contract to support the tasks of this contract. Service Contract Labor Standards (SCLS) Wage Determination (WD) codes are provided as applicable. See **Attachment B: Wage Determinations (2015-4269 and 2015-4281)**.

G.5 AVAILABILITY OF FUNDS

The Government's obligation for performance of this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract until funds are made available to the CO for performance and until the Contractor receives notice of availability, to be confirmed in writing by the CO.

The \$10,000.00 guaranteed minimum of this IDIQ contract is anticipated to be obligated at time of IDIQ award.

G.6 GOVERNMENT POINTS OF CONTACT

IDIQ Contracting Officer (CO)

- Name and Position: Nicholas Bisher, Lead Contract Specialist
- Office: Office of Operations (OO)/ Office of Finance, Budget, and Acquisitions (OFBA)/ Office of Acquisitions and Grants Services (OAGS)/ Division of Acquisition Operations (DAO)/ Service Contracts Branch (SCB)
- Phone: 240-402-2773
- Email: Nicholas.Bisher@fda.hhs.gov

IDIQ Contract Specialist (CS)

- Name and Position: Melinda Kim, Contract Specialist
- Office: OO/OFBA/OAGS/DAO/SCB
- Phone: 301-796-0607
- Email: Melinda.Kim@fda.hhs.gov

IDIQ Contracting Officer's Representative (COR)

- Name and Position: *To be determined at time of award*
- Office: *To be determined at time of award*
- Phone: *To be determined at time of award*
- Email: *To be determined at time of award*

G.7 CONTRACTING OFFICER'S AUTHORITY

The Contracting Officer (CO) is the only individual who has the authority to enter into, administer, or terminate this contract and is the **only person authorized** to approve changes to any of the requirements under this contract. It is the Contractor's responsibility to contact the CO immediately if there is even the appearance of any technical direction that is, or may be, outside the scope of the contract. In the event the Contractor effects any changes to this contract or contracts at the direction of any person other than the CO, the changes will be considered to have been made without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof. The CO will be the only individual authorized to accept nonconforming work, waive any requirement of the contract/task order and modify any term or condition of the contract/task order. The Contracting Officer is the only individual who can legally obligate Government funds. No costs chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

Only the Contracting Officer has authority to: (1) direct or negotiate any changes in the statement of work; (2) modify or extend the period of performance; (3) change the delivery schedule; (4) authorize reimbursement to the Contractor any costs incurred during the performance of this contract; or (5) otherwise change any terms and conditions of this contract.

G.8 CONTRACTING OFFICER'S REPRESENTATIVE'S AUTHORITY

The Contracting Officer (CO) may designate other Government personnel, known as the Contracting Officer's Representative (COR) to act as his or her authorized representative for contract administration functions which do not involve changes to the scope, price, schedule, or terms and conditions of the contract. The designation will be in writing, signed by the Contracting Officer, and will set forth the authorities and limitations of the representative(s) under the contract. Such designation will not contain authority to sign contractual documents, order contract changes, modify contract terms, or create any commitment or liability on the part of the Government different from that set forth in the contract. CORs do not have authority to act as agent of the Government under the contract or task order.

At any time, the Government may unilaterally change its COR designation without prior notice to the Contractor by

a unilateral modification that is signed only by the CO in accordance with RFO FAR 43.203(b) (June 12, 2025) [adopted via HHS FAR CD 2025-05 (July 21, 2025)].

The IDIQ COR, to be designated at time of contract award, will represent the Government for the purpose of the IDIQ. The IDIQ COR will be responsible for the following:

- Tracking compliance with Limitations on Subcontracting clause across task orders
- Tracking and monitoring contract ceiling
- Tracking and monitoring staff allocation across task orders
- Reviewing changes to staffing matrix
- Secondary point of contact for issues that need to be escalated
- Reviewing Task Order SOWs for scope compliance
- Completing annual CPARS evaluations

G.9 TECHNICAL DIRECTION

Performance of the work under this contract shall be subject to the technical direction of the IDIQ COR. The term “technical direction” is defined to include, without limitation, the following:

- Directions to the Contractor which redirect the contract effort, shift work emphasis between work areas or tasks, require pursuit of certain lines of inquiry, fill in details or otherwise serve to accomplish the contractual statement of work.
- Provision of information to the Contractor which assists in the interpretation of drawings, specifications, or technical portions of the work description.
- Review and, where required by the contract, approval of technical reports, drawings, specifications, and technical information to be delivered by the Contractor to the Government under the contract.

Technical direction must be within the general Scope of Work stated in the contract. The IDIQ COR does not have the authority to and may not issue any technical direction which:

- Constitutes an assignment of additional work outside the general Scope of Work of the contract.
- Constitutes a change as defined in the applicable contract clause:
 - “Changes” paragraph (d) within RFO FAR clause 52.212-4 TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES, ALTERNATE I (DEVIATION DATE) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]
 - RFO FAR clause 52.243-1 CHANGES-FIXED PRICE, ALTERNATE III (DEVIATION DATE) [HHS FAR CD 2025-05 (Jul. 21, 2025), RFO FAR 43.305(a)(2) (Jun. 12, 2025), RFO FAR 52 (July 1, 2026)]
 - RFO FAR clause 52.243-3 CHANGES-TIME-AND-MATERIALS OR LABOR-HOURS (DEVIATION DATE) [HHS FAR CD 2025-05 (Jul. 21, 2025), RFO FAR 43.305(c) (Jun. 12, 2025), RFO FAR 52 (July 1, 2026)]
- Change any of the expressed terms, conditions, or specifications of the contract.

All technical direction will be issued in writing by the IDIQ COR or will be confirmed by him/her in writing within five (5) business days after issuance.

If, in the opinion of the Contractor, any instructions or direction issued by the IDIQ COR is within one of the categories described above, the Contractor shall not proceed but shall notify the IDIQ CO in writing within five (5) working days after the receipt of any such instructions or direction and shall request the CO to modify the TO, accordingly. Upon receiving such notification from the Contractor, the IDIQ CO will issue an appropriate contract modification or advise the Contractor in writing that, in his/her opinion, the technical direction is within the scope of this contract. The Contractor shall proceed immediately with the instructions or directions and shall be subject to the “Disputes” paragraph (e) within RFO FAR clause 52.212-4(d), Terms and Conditions—Commercial Products and Commercial Services (Deviation Date).

G.10 TASK ORDER (TO) CONTRACTING OFFICER'S REPRESENTATIVES (CORs)

For each individual task order, a Task Order (TO) Contracting Officer's Representative (COR) will be assigned with the same authorities as the IDIQ COR for each individual TO. The TO COR will serve as the Contractor's first point of contact for any technical questions and is responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and compliance with all substantive project objectives; (2) interpreting the statement of work and any other technical performance requirements; (3) performing technical evaluation as required; (4) performing technical inspections and acceptances required by this contract; (5) assisting in the resolution of technical problems encountered during performance; and (6) providing technical direction; and, (7) reviewing and approving invoices/vouchers.

G.11 TASK ORDER PROJECT MANAGERS (TOPMs)

Task Order Project Managers (TOPMs) may assist the CORs, but will not have the authority to provide technical direction as described in Section G.9; however, they may be responsible for: (1) monitoring the Contractor's technical progress, including the surveillance and assessment of performance and compliance with all substantive project objectives; (2) performing technical evaluation as required; (3) performing technical inspections and acceptances then reporting to the COR of the acceptance as required by this performance; and (4) reviewing of invoices/vouchers.

G.12 TRAVEL

No travel is anticipated under this contract. Any travel costs incurred by the Contractor within the Washington, D.C. metropolitan area, including to/from the Contractor's FIRF facility, shall be considered local travel and will not be reimbursed.

If necessary, individual task orders may include travel. All travel must be pre-negotiated in individual task orders and approved and authorized by the Task Order COR. Travel will be reimbursed in accordance with the Federal Travel Regulation (FTR), set forth at Title 41, Subtitle F, chapters 300 through 304, of the Code of Federal Regulations. Travel requirements under this contract shall be met using the most economical form of transportation available. If economy class transportation is not available, the request for payment voucher must be submitted with justification for use of higher-class travel indicating dates, times, and flight numbers. All travel shall be scheduled sufficiently in advance to take advantage of offered discount rates, unless otherwise directed by the Contracting Officer.

G.13 OTHER DIRECT COSTS (ODCs)

Allowable Other Direct Costs (ODCs) in support of specific task orders shall be proposed and will be evaluated at the task order level.

Any ODCs shall be submitted through the invoice. All ODCs over \$3,000, other than those ODCs acquired under the firm-fixed price line items, must be pre-approved by the Contracting Officer, if not already approved through the issuance of a task order or modification.

To be eligible to receive reimbursement for ODCs, the Contractor must obtain at least three (3) quotes for each transaction in excess of \$3,000.00 to ensure that adequate price competition was sought, or the Contractor must provide an acceptable justification as to why it was impracticable to do so. For purchases of ODCs, the Contractor shall provide the aforementioned documentation only when requested by the Contracting Officer.

The Contractor shall maintain documentation of all reimbursable purchases until three (3) years after the contract is completed and shall provide access to and copies of such documentation, when requested by the Contracting Officer.

G.14 INVOICING INSTRUCTIONS AND REQUIREMENTS

Specific invoicing instructions may be provided in each individual task order. Unless otherwise specified in the task order, the FDA Invoicing procedures are as follows:

DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ACQUISITION REGULATION (HHSAR) 352.232-71 – ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (APR 2026) (RFO DEVIATION) [HHSAR CD 2026-07 (Apr. 23, 2026)]

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

Payment request means a bill, voucher, invoice, or request for contract financing payment with associated supporting documentation. The payment request must comply with the requirements in FAR 32.905(b) and the applicable payment clause included in this contract.

(b) *Submission instructions.* Except as provided in paragraph (c) of this clause, the Contractor must submit payment requests electronically using the Department of Treasury Invoice Processing Platform (IPP) or successor system. Information regarding IPP, including IPP Customer Support contact information, is available at www.ipp.gov or any successor site.

(c) *Alternate submission procedures.* The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing.

(d) *Submission of alternate payment procedures authorization.* If alternate payment procedures are authorized, the Contractor must include a copy of the Contracting Officer's written authorization with each payment request.

(End of clause)

FDA Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP) (Jan 2022)

a. All Invoice submissions for goods and or services must be made electronically through the U.S. Department of Treasury's Invoice Processing Platform System (IPP). <http://www.ipp.gov/vendors/index.htm>

b. Invoice Submission for Payment means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in FAR 32.905(b), "Content of Invoices" and the applicable Payment clause included in this contract, or the clause FAR 52.212-4 Contract Terms and Conditions - Commercial Items included in commercial items contracts. The IPP website address is: <https://www.ipp.gov>.

c.

1. The Agency will enroll the Contractors new to IPP. The Contractor must follow the IPP registration email instructions for enrollment to register the Collector Account for submitting invoice requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive Registration email from the Federal Reserve Bank of St. Louis (FRBSTL) within 3 - 5 business days of the contract award for new contracts or date of modification for existing contracts.

2. Registration emails are sent via email from ipp.noreply@mail.eroc.twai.gov. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email to IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973-3131.

3. The Contractor POC will receive two emails from IPP Customer Support, the first email contains the initial administrative IPP User ID. The second email, sent within 24 hours of receipt of the first email, contains a temporary password. You must log in with the temporary password within 30 days.

4. If your company is already registered to use IPP, you will not be required to re-register.

5. If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment as authorized by HHSAR 332.7002, a written request must be submitted to the Contracting Officer to explain the circumstances that require the authorization of alternate payment procedures.

d. Invoices that include time and materials or labor hours Line Items must include supporting documentation to (1) substantiate the number of labor hours invoiced for each labor category, and (2) substantiate material costs incurred

(when applicable).

e. Invoices that include cost-reimbursement Line Items must be submitted in a format showing expenditures for that month, as well as contract cumulative amounts. At a minimum the following cost information shall be included, in addition to supporting documentation to substantiate costs incurred:

- Direct Labor - include all persons, listing the person's name, title, number of hours worked, hourly rate, the total cost per person and a total amount for this category;
- Indirect Costs (i.e., Fringe Benefits, Overhead, General and Administrative, Other Indirects)- show rate, base and total amount;
- Consultants (if applicable) - include the name, number of days or hours worked, daily or hourly rate, and a total amount per consultant;
- Travel - include for each airplane or train trip taken the name of the traveler, date of travel, destination, the transportation costs including ground transportation shown separately and the per diem costs. Other travel costs shall also be listed;
- Subcontractors (if applicable) - include, for each subcontractor, the same data as required for the prime Contractor;
- Other Direct Costs - include a listing of all other direct charges to the contract, i.e., office supplies, telephone, duplication, postage; and
- Fee - amount as allowable in accordance with the Schedule and FAR 52.216-8 if applicable.

f. Contractor is required to attach an invoice log addendum to each invoice which shall include, at a minimum, the following information for contract administration and reconciliation purposes:

(a) list of all invoices submitted to date under the subject award, including the following:

- (1) invoice number, amount, & date submitted
- (2) corresponding payment amount & date received

(b) total amount of all payments received to date under the subject contract or order

(c) and, for definitized contracts or orders only, total estimated amounts yet to be invoiced for the current, active period of performance.

g. Payment of invoices will be made based upon acceptance by the Government of the entire task or the tangible product deliverable(s) invoiced. Payments shall be based on the Government certifying that satisfactory services were provided, and the Contractor has certified that labor charges are accurate.

h. If the services are rejected for failure to conform to the technical requirements of the task order, or any other contractually legitimate reason, the Contractor shall not be paid, or shall be paid an amount negotiated by the CO.

i. Payment to the Contractor will not be made for temporary work stoppage due to circumstances beyond the control of U.S. Food and Drug Administration such as acts of God, inclement weather, power outages, and results thereof, or temporary closings of facilities at which Contractor personnel are performing. This may, however, be justification for excusable delays.

j. The Contractor agrees that the submission of an invoice to the Government for payment is a certification that the services for which the Government is being billed, have been delivered in accordance with the hours shown on the invoices, and the services are of the quality required for timely and successful completion of the effort.

k. Questions regarding invoice payments that cannot be resolved by the IPP Helpdesk should be directed to the FDA Employee Resource and Information Center (ERIC) Helpdesk at 301-827-ERIC (3742) or toll-free 866-807-ERIC (3742); or, by email at ERIC@fda.hhs.gov. Refer to the Call-in menu options and follow the phone prompts to dial the option that corresponds to the service that's needed. All ERIC Service Now Tickets will either be responded to or resolved within 48 hours (2 business days) of being received. When emailing, please be sure to include the contract number, invoice number and date of invoice, as well as your name, phone number, and a detailed description of the issue.

G.15 CONTRACT FINANCIAL REPORTING

Financial reports shall be submitted by the contractor with the invoices for Time-and-Materials (T&M) and Labor-Hour (LH) type Task Orders in accordance to the expenditure categories below:

- Accumulate total for all cost categories (i.e., labor, travel)
- Contract ceiling and percent expended to date
- Estimate to complete
- Travel – Include all direct costs to travel, including transportation subsistence and miscellaneous expenses. The following information shall be submitted: Name of traveler and purpose of trip; Place of departure,

destination and return, including time and dates; and total cost of trip. The Contractor will be reimbursed for travel expenditures incurred as a direct cost during performance of defined requirements stated in orders in accordance with the appropriate limitations set forth in RFO FAR 31.205-46 (July 17, 2025) [adopted via HHS FAR CD 2025-06 (Aug. 1, 2025)].

G.16 GOVERNMENT FURNISHED PROPERTY (GFP)

Specific Government furnished property will be identified within each individual TO.

The contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation or rehabilitation costs.

The Contractor shall return all Government furnished property to the COR no later than the expiration date of this contract or any TO.

Government furnished property (materials, equipment, and/or information) will be provided in conjunction with required performance under this contract, as determined by mutual agreement between FDA and the Contractor.

When the Government provides equipment, the Contractor shall maintain a detailed inventory accounting system for Government Furnished Property (GFP) following contract award. The inventory accounting system must specify, at a minimum:

- Product description (make, model)
- Government tag number
- Date of receipt
- Name of receipt
- Location of receipt
- Current location
- Contract/order number under which the equipment is being used

The Contractor shall attach an update inventory report to each Monthly Progress Report unless otherwise specified by the COR. In either case, the Contractor's inventory listing must be available for Government review within one (1) business day of COR request. The Contractor shall remain responsible and accountable for all GFP for the duration of the contract and ensure the return of the property upon completion of all work required under this contract.

CDRH Property Custodian:

Name: Deborah Ward
Address: U.S. Food and Drug Administration
White Oak Campus, Building 66
10903 New Hampshire Ave
Silver Spring, Maryland 20993
Phone: 301-796-4771
Email: Deborah.Ward@fda.hhs.gov

All property, data and information provided by the Government in the performance of this contract remains the property of the Government and shall be surrendered to the Government upon completion or termination of this contract. Likewise, all deliverables generated under this contract remain the property of the Government.

Upon award of this contract, the Government will provide the following to the contractor:

- Laptop computer with standard office software and internet access for the performance of the above duties.
- FDA Personal Identity Verification (PIV) card (badge)

In addition to the requirements of FAR clause 52.245-1 GOVERNMENT PROPERTY (Sept 2021), incorporated in Section I of this contract, the Contractor shall comply with the provisions of HHS Publication, "[HHS Contracting Guide for Contract of Government Property](#)," which is incorporated into this contract by reference.

G.17 GOVERNMENT FURNISHED EQUIPMENT (GFE)

The FDA may provide laptops, tower computers, printers, scanners, copier, data cable line, and basic PC desktop images and Center Software Top-Offs for FIRF in individual TOs. Upon receipt of FDA badges, FDA will provide Contractor FDA network access to staff under this contract. FDA will provide access to any server-based environment necessary to accomplish the stated work.

The Contractor shall work with the FDA Help Desk Support to relocate/install all Government Furnished Equipment (GFE) to ensure no breaks in current work performance.

Upon the expiration of the one-year manufacturer's warranty for the GFE, the Contractor shall be responsible for maintaining all GFE equipment in accordance with current commercial operating standards until replaced or returned to the FDA.

The Contractor shall be responsible for providing any supplies necessary to operate the GFE (other than maintenance/repair supplies).

G.18 FDA INFORMATION TECHNOLOGY (IT) HELP DESK SUPPORT

Help Desk Support will be provided by the FDA for only FDA functions inclusive of support for all Government Furnished Property (GFP) and software. FDA's Help Desk is responsible for distributing new and replacement laptops as they are needed and configuring laptops with standard and Center specific software. FDA Help Desk Support will be provided through remote access, drop-in support, or when the Contractor transports the equipment to the nearest FDA IT servicing location. Drop-in support services include: transition-in services and support for major technology changes that cannot efficiently be accomplished remotely. Upon request by FDA Help Desk Support, the Contractor shall be responsible for transporting the items in need of repair to and from the designated FDA facility for repair. In addition, the FDA's Help Desk provides best effort support – defined as basic troubleshooting - for peripheral equipment connected to FDA owned computers. FDA does not grant the Contractor administrative rights for Government- owned computers. If required, the Contractor shall submit a request for administrative rights using the Form 3530 and submit to FDA for approval.

G.19 GOVERNMENT FURNISHED INFORMATION

Government Furnished Information will be accessible through the FDA network and paper copies, as needed. The Contractor shall inform and require staff to comply with Government regulations that prohibit the use of any Government property for personal use.

The FDA will not supply the Contractor with phones. The FDA will provide the data drops (if not pre- existing or extras are needed) and network infrastructure (e.g., DS3 circuit, network switch, network router) for connection to the FDA network, via the Verizon direct connection between the Contractor's FIRF facility and the FDA White Oak Campus.

G.20 CONTRACTOR EQUIPMENT REQUIREMENTS

The FDA Master Approved Technology (MAT) list contains a list of software applications and equipment approved by the Office of Information Management and Technology (OIMT). The approved technologies are determined to be compatible with FDA's Technical environment. The MAT list is posted on FDA's intranet and will be available to authorized Contractor employees after contract award. In addition, FDA posts a list of technologies not approved by OIMT on the intranet.

All Contractor peripheral equipment connected to FDA computers or laptops must be on the MAT List. If Contractor equipment and software is not on the MAT List (as determined after contract award), it must be approved via the formal FDA technical approval process prior to connection to FDA's network.

The Contractor shall be responsible for identifying needed technologies that are not provided by the FDA. FDA has instituted the Information Technology Information Management (ITIM) approval process in order to track technologies across the Agency. The introduction of a new technology or a different version of an already approved technology requires the submission and approval of an ITIM request. The Contractor may be responsible for supporting the ITIM process including writing and submitting ITIM requests and tracking them from inception through completion. FDA Center IT Investment Review Boards may need to be included in a coordinated review process.

G.21 GOVERNMENT FURNISHED DATA

The Government shall retain all rights and privileges, including those of patent and copy, to all Government-furnished data and materials. The Contractor shall neither retain nor reproduce for private or commercial use any data or other materials furnished under this contract. The Contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are beyond any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract.

G.22 POST-AWARD EVALUATION OF CONTRACTOR PERFORMANCE

Contractor Performance Evaluations

Interim and final evaluations of contractor performance will be prepared on this contract in accordance with RFO FAR 42.11 (Sept. 30, 2025) [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)]. The final performance evaluation will be prepared at the time of completion of work. In addition to the final evaluation, interim evaluations will be prepared annually to coincide with the anniversary date of the contract.

Interim and final evaluations will be provided to the Contractor as soon as practicable after completion of the evaluation. The Contractor will be permitted thirty (30) days to review the document and to submit additional information or a rebutting statement. If agreement cannot be reached between the parties, the matter will be referred to an individual one level above the Contracting Officer, whose decision will be final.

Copies of the evaluations, contractor responses, and review comments, if any, will be retained as part of the contract file, and may be used to support future award decisions.

Electronic Access to Contractor Performance Evaluations

Contractors that have internet capability may access evaluations through a secure website for review and comment by completing the registration form that can be obtained at the following address:
<https://www.cpars.gov/cparsweb/home>.

The registration process requires the Contractor to identify an individual that will serve as a primary contact and who will be authorized access to the evaluation for review and comment. In addition, the Contractor will be required to identify an alternate contact that will be responsible for notifying the cognizant contracting official in the event the primary contact is unavailable to process the evaluation within the required 30-day time frame.

Section H. Special contract requirements

H.1 ACCOUNTABILITY AND SECURITY

All Contractor and subcontractor employees who will have access to Government information and/or sensitive materials must sign a Contractor's Commitment to Protect Non-Public Information (NPI) Agreement (Form FDA 3398), available as **Attachment H**. It is the responsibility of the Contractor to assure that such Agreements have been signed before access is permitted. Copies of signed agreements must be provided to the Contracting Officer's Representative (COR).

The following procedures and rules shall be followed by the Contractor according to the Privacy Act of 1974, as amended, and the FDA security and confidentiality procedures applicable to this contract:

- A. All information and reports generated from this project are, and will remain, the property of the FDA. No Government document or information, oral or written, either in final or draft form, will be provided to non-FDA sources by any Contractor personnel without the written approval of the Contracting Officer during this contract or at any later date.
- B. No data covered by privacy laws may leave the United States for any purpose or under any circumstances unless prior approval by the Contracting Officer is first obtained.
- C. The Contractor must ensure that all FDA data or documents processed or developed under this contract, and the information contained therein, are protected from unauthorized use and mishandling by assigned personnel.
- D. There shall be no dissemination or publication, except within and between Contractor personnel, of information developed under this contract or contained in the reports to be furnished pursuant to this contract, without the prior written approval of the Contracting Officer. Further, the Contractor shall not reveal, during the performance of this contract or later, any of the operating methods or systems, contents of files, names of persons, firms, or places mentioned under the contract that the Contractor may acquire, unless approved in writing by the Contracting Officer.
- E. Under the provisions of the Privacy Act of 1974, as amended, that is applicable to this contract, the Contractor and Contractor personnel may be subject to its criminal penalties. The Contractor agrees that, upon termination of the contract, whether with or without cause, the Contractor has no property or possessor right to any of the correspondence, files or materials, of whatever kind and description, or any copies or duplicates of such, whether developed/prepared by the Contractor or furnished to the Contractor by the technical office concerning the performance of this contract; and that, upon demand, the Contractor will surrender immediately to the Contracting Officer such items, matters, materials, and copies. A restraining order or an injunction may be issued against the Contractor for any violation of this provision, besides any other right or penalty by law that the Government may have.

The above terms and conditions of this contract clause are subject to formal modification or amendment by the Government in those instances in which the courts (e.g., grand jury investigations), statutory requirements (e.g., civil investigative demands), or specific circumstances dictate such changes.

H.2 DATA RIGHTS

All data, code, designs and other documents and project artifacts created and/or gathered in the course of the project shall be transferred to the U.S. Government agency as set forth in FAR clause 52.227-17 Rights in Data—Special Works (DEC 2007). The Contractor shall not publicize or disseminate information obtained through this order without the prior written approval of the Government. In addition, the Contractor shall not mark data/deliverables created and/or gathered in the course of this project as with their company's imprint as proprietary.

H.3 CONTRACTOR ADVERTISING OF CONTRACT AWARD

The Contractor shall not refer to the product or service awarded under this contract in commercial advertising, as defined in RFO FAR 31.205-1 (July 17, 2025) [adopted via HHS FAR CD No. 2025-06 (Aug. 1, 2025)], in any

manner which states or implies the U.S. Food and Drug Administration's approval or endorsement of the product or service being provided; or, states or implies that the product or service being provided is considered to be superior to other industry products or services. The Contractor may request the Contracting Officer to make a determination as to the propriety of promotional material.

H.4 NON-PERSONAL SERVICES AND INHERENTLY GOVERNMENTAL FUNCTIONS

Pursuant to RFO FAR 37.2 (Sept. 25, 2025) [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)], no personal services shall be performed under this contract. No Contractor employee will be directly supervised by the Government. All individual employee assignments, and daily work direction, shall be given by the applicable employee supervisor. If the Contractor believes any Government action or communication has been given that would create a personal services relationship between the Government and any Contractor employee, the Contractor shall promptly notify the Contracting Officer of this communication or action.

The Government and the Contractor understand and agree that the services delivered by the Contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee relationship will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement to benefits given Federal employees.

Contractor personnel under this contract shall not:

- Be placed in a position where there is an appearance that they are employed by a Federal Officer, or are under the supervision, direction, or evaluation of a Federal Officer.
- Be placed in a position of command, supervision, administration, or control over personnel or personnel of other Government contractors or become a part of the Government organization.
- Be used in administration or supervision of procurement activities.

Pursuant to RFO FAR 7.5 (Sept. 4, 2025) [adopted via HHS FAR CD 2025-11 (Nov. 3, 2025)], the Contractor shall not perform any inherently governmental actions under this contract. No Contractor employee shall hold him or herself out to be a Government employee, agent, or representative. No Contractor employee shall state orally or in writing at any time that he or she is acting on behalf of the Government. In all communications with third parties in connection with this contract, Contractor employees shall identify themselves as Contractor employees and specify the name of the company for which they work. In all communications with other Government contractors in connection with this contract, the Contractor employee shall state that they have no authority to in any way change the contract and that if the other contractor believes this communication to be a direction to change their contract, they should notify the Contracting Officer for that contract and not carry out the direction until a clarification has been issued by the Contracting Officer.

The Contractor shall ensure that all of its employees working on this contract are informed of the substance of this article. Nothing in this article shall limit the Government's rights in any way under the other provisions of the contract, including those related to the Government's right to inspect and accept the services to be performed under this contract. The substance of this article shall be included in all subcontracts at any tier.

H.5 REPORTING MATTERS INVOLVING FRAUD, WASTE, AND ABUSE

Anyone who becomes aware of the existence or apparent existence of fraud, waste and abuse in FDA funded programs is encouraged to report such matters to the HHS Inspector General's Office in writing or on the Inspector General's Hotline. The toll-free number is **1-800-HHS-TIPS (1-800-447-8477), 8:00 am – 5:30 pm Eastern Time, Monday –Friday. Fax 1-800-223-8164, TTY 1-800-377-4950.** All telephone calls will be handled confidentially. The e-mail address is hhstips@oig.hhs.gov and the mailing address is:

HHS TIPS Hotline
TIPS HOTLINE
P.O. Box 23489
Washington, D.C. 20026

H.6 IDENTIFICATION OF CONTRACTOR EMPLOYEES

During the period of performance of this contract, the rights of ingress and egress to and from any Government office for Contractor representatives shall be made available as required. All Contractor employees whose duties under this contract require their presence at any Government facility shall be clearly identifiable by a distinctive badge furnished by the Government. All prescribed information shall immediately be delivered to the FDA Personnel Security Branch for cancellation or disposition upon the termination of the employment of any Contractor personnel. All on-site Contractor personnel shall abide by security regulations applicable to that site.

H.7 ORGANIZATIONAL CONFLICTS OF INTEREST

As a regulatory agency charged with protection of the public health, the U.S. Food and Drug Administration (FDA) must maintain public confidence in the integrity of its decisions. The FDA has various policies and procedures that safeguard against both actual and apparent conflict of interest (COI) on the part of its employees. It is additionally critical that the FDA be assured that there is not actual or apparent COI on the part of either the Contractor's organization or its individual employees in performance of this contract action.

The Contractor must ensure the protection of the information and data it receives in performance of this contract from unauthorized use or disclosure and must avoid actions that would cause a reasonable person to question the impartiality of the Contractor, its employees, or the Government in the performance of this immediate contract and potential participation in future actions. The Contractor will be held to the restrictions of the Organizational Conflict of Interest clause, unless an acceptable mitigation of risk plan is proposed, is found acceptable by the Government and enforced.

POTENTIAL CONFLICTS OF INTEREST SPECIFIC TO THIS CONTRACT - The Contractor shall review the Statement of Work included in this contract in detail to identify any particular aspects that may present organizational or individual COI, either actual or apparent.

DEFINITION OF CONFLICT OF INTEREST - *Organizational conflict of interest* means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage (see FAR part 2, Definitions of Words and Terms).

Organizational Conflict of Interest/Do Not Compete

- a. The Contractor and all of its present and future affiliates and subsidiaries agree to:
 - 1) not compete nor assist anyone in competing for any competitive acquisition of the requirements or services described in the documents which the Contractor has been provided access to or delivers under this contract and contracts thereof.
 - 2) not furnish either as a prime contractor or subcontractor the requirements or services described in paragraph a.1) above.
- b. The above prohibitions shall also apply to the Contractor's employees, subcontractors, consultants or any other person who participates in the performance of this contract. The Contractor shall require such persons to sign the below statement agreeing to the above restrictions. The original of the below statement shall be provided to the Contracting Officer, prior to the person beginning work under this contract/order.
- c. Noncompliance with the above restrictions and conditions shall be a cause for: termination of this contract for default; and/or, disqualification of any proposal submitted for a competition.

ORGANIZATIONAL CONFLICT OF INTEREST STATEMENT
FDA IDIQ Contract No. TBD

(Type name of employee), an employee of (Type name of Contractor), agrees to:

1. not compete nor assist anyone in competing for any competitive acquisition of the requirements or services described in the documents which the contractor has been provided access to or delivers under this contract; specifically, the documents, process, and forms of the Center for Devices and Radiological Health (CDRH).
2. not furnish either as an employee of a prime contractor or subcontractor the requirements or services described in paragraph 1) above.

Signature

Date

H.8 FDA 1350 ACCESS TO NON-PUBLIC INFORMATION

All Contractor and subcontractor employees are required to sign the Contractor's Commitment to Protect Non-Public Information (NPI) Employee Agreement (Form FDA 3398), provided as **Attachment H** to this contract. If a person who has signed this agreement resigns, is dismissed, or is otherwise no longer working on this contract, the Contractor shall notify the FDA Project Officer and the Contracting Officer. Any new Contractor or subcontractor employee assigned to this contract shall sign the form, and the Contractor shall electronically deliver it to the Contracting Officer ten (10) days prior to said new employee's commencement of work on this contract.

The prime Contractor, subcontractors, and consultants shall not be provided nor possess non-public information in any form unless written approval has been granted, nor shall they have unaccompanied access to an FDA facility unless a facility clearance has been granted.

H.9 BRIEFINGS

An FDA representative (typically, the Contracting Officer's Representative) will conduct an orientation briefing for the Contractor and subcontractor employees. The briefing will stress: (1) the importance of protecting non-public information; (2) specified computer/IT requirements as outlined in the DHHS Automated Information Systems Security Program Handbook; and (3) the consequences of unauthorized disclosure of non-public information. Briefing updates will be conducted annually.

The Contractor shall brief all Contractor employees, subcontractors and consultants regarding the sensitivity of the information to be handled under the contract and of their responsibility to protect it. The briefing shall stress that the information is non-public and shall not be disclosed to any unauthorized party. The Contractor shall conduct an updated briefing annually and shall submit a report to the FDA Project Officer within ten (10) days after the briefing which includes: an outline of the briefing; copies of any briefing materials; the date the briefing was conducted; and the names of the attendees.

If this is an information technology/telecommunication (IT/TC) contract, in addition to the above briefings, the FDA COR and the FDA Center/Office Information Systems Security Officer (ISSO) will brief Contractor and subcontractor personnel on security measures required pertinent to any hardware/software being utilized. Furthermore, appropriate Contractor and subcontractor personnel shall attend training courses as directed by the FDA to fulfill requirements of the Computer Security Act of 1987. These courses are generally one (1) day in length, and attendance at one (1) course is sufficient. This training will be provided at no cost to the Contractor.

H.10 NOTICE TO THE GOVERNMENT OF DELAYS

In the event the Contractor encounters difficulty in meeting performance requirements, or when the Contractor anticipates difficulty in complying with the contract delivery schedule or completion date, or whenever the Contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the Contractor shall immediately notify the Contracting Officer and COR in writing, giving pertinent details. This data shall be informational only in character and this provision shall not be construed as a waiver by the Government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

H.11 PERSONNEL

The Contractor shall ensure that all Contractor support personnel are adequately trained, possess the credentials specified in the appropriate labor categories, and are otherwise fully qualified to provide the high level of support required by this contract prior to being assigned to the awarded contract.

H.12 GOVERNMENT-FURNISHED DATA AND MATERIALS

The Government shall retain all rights and privileges, including those of patent and copy, to all Government-furnished data and materials. The Contractor shall neither retain nor reproduce for private or commercial use any

data or other materials furnished under this contract. The Contractor agrees not to assert any rights at common law or in equity or establish any claim to statutory copyright in such data. These rights are not exclusive and are beyond any other rights and remedies to which the Government is otherwise entitled elsewhere in this contract.

H.13 TRANSITION

The Contractor shall provide all management, administrative, clerical, and supervisory functions required for the effective and efficient performance of this contract.

A smooth and orderly transition between the Contractor and a predecessor or successor Contractor is necessary to ensure minimum disruption to vital Government business. The Contractor shall cooperate fully in the transition. The Contractor shall adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall NOT:

- Discuss with unauthorized persons any information obtained in the performance of work under this contract;
- Conduct business not directly related to this contract on Government premises;
- Use computer systems and/or other Government facilities for company or personal business other than work related to this contract; or
- Recruit on Government premises or otherwise act to disrupt official Government business.

It is the Government's intention to perform closeout procedures on an individual contract basis. The Contractor agrees to perform those internal functions necessary to support this process in a timely manner. The contract closeout will occur as soon as possible after required audit and establishment of final rates, as applicable.

H.14 INSURANCE REQUIREMENTS

The Contractor shall maintain the types of insurance and coverage required in RFO FAR 28.3 (Aug. 28, 2025) [adopted via HHS FAR CD 2025-11 (Nov. 3, 2025)], and per FAR clause 52.228-5, Insurance – Work on a Government Installation (Jan 1997).

Upon contract award, the contractor shall furnish to the Contracting Officer a certificate or written statement of insurance prior to commencement of work under this contract. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness and contract number. The contract number and task order number (if applicable) shall be cited on the certificate of insurance.

H.15 ADDITIONAL SECURITY AND CONFIDENTIALITY REQUIREMENTS

The Contractor shall realize the regulatory nature of the FDA and accept responsibility for exercising diligence in protecting the security and confidentiality of any information acquired with the FDA networking infrastructure, staff projects, meetings, seminars, or other sensitive information.

During the course of the contract, if questions arise as to what information can be shared with potential solution providers, others performing maintenance on systems, third party or other staff, the contractor will seek guidance and approval from the COR.

H.16 CONTRACTOR CONFORMANCE WITH APPLICABLE LAWS, REGULATIONS, POLICIES, AND STANDARDS

The Contractor shall be responsible for knowledge of and compliance with all applicable federal information technology and information management laws, regulations, policies, and standards at the Government-wide, HHS and FDA levels.

H.17 HANDLING OF NON-PUBLIC RECORDS MATERIAL

The following clause may be applicable at the Task Order level.

Accountability of Non-Public Information (NPI) is essential to maintaining a history of what an organization has and where NPI is located. Through effective accounting procedures, it must be possible to trace the movement and detect the loss of NPI in a timely manner. Adequate accountability record systems shall be in place to track NPI received, generated, transmitted or destroyed.

Inventories. Periodic inventories shall be conducted for all NPI documents. Inventory record shall be retained until the next inventory has been completed.

Report of Lost Documents. All physical losses of NPI shall be reported to the FDA Physical Security Staff, the Assistant Records Liaison Officer (ARLO), IDIQ COR, and TO COR. The report shall include the identification and description of the missing document(s), the name and organizational location of the individual to whom the document(s) were last charged, and a summary of the efforts made to locate the missing document(s). Contractors are responsible for following supplemental instructions for reporting lost documents as identified in ITO's. Contractors shall make every reasonable effort to comply with NPI policies as identified in this contract.

Storage. During working hours, individuals shall take all necessary precautions to prevent access to NPI by unauthorized persons (i.e., persons who do not possess an appropriate security clearance and/or who do not possess the required need-to-know). Emphasis shall be placed on administrative safeguards and individual security responsibilities during normal working hours. NPI documents, when removed from storage for working purposes, shall be kept under constant surveillance and turned face-down or covered when not in use. NPI documents shall not be left unattended. If this is not possible, the safeguarding requirements for after working hours apply. NPI created on automated information systems are susceptible to interception by unauthorized persons due to the compromising emanations threat. Computers used frequently to handle NPI shall have a reduced level of emanations or located in an area with sufficient perimeter of control. Computers used to handle NPI shall have the proper safeguards to ensure that all data is protected from disclosure. All system vulnerabilities must be identified, and the risk minimized. After working hours, NPI documents shall be stored in approved secure file areas or containers.

Recalled Documents. NPI documents retrieved/recalled from storage at the Federal Records Center shall be provided the same protection they received before transfer to the Center. All recalled documents shall be entered in their accountability system. Accountability and safeguarding requirements shall continue until the documents are returned to the Federal Records Center or disposed of by other means, e.g., destroyed.

Contractor Facility. Storage locations at a Contractor facility shall be approved (in writing) by the FDA Physical Security Staff (HFA-204).

Transmission. NPI shall be transmitted either in the custody of an appropriately cleared and authorized individual (preferred method) or by an approved system or carrier (with signature receipt), as outlined below:

Courier/Personal Delivery. Individuals delivering NPI documents shall be briefed on their responsibilities on security precautions to prevent the unauthorized disclosure of the information until the delivery is complete. Documents shall remain in the physical possession of the individual delivering the NPI at all times. Documents shall not be read, studied, displayed, discussed or used in any manner in public places.

Mail. U.S. Registered/Certified, or commercial carrier express mail (with signature receipt) may be used for the transmission of NPI (paper copies, disks, CDs, or other media in hard copy form).

Fax. NPI documents may be transmitted via the fax machine only upon verification that the intended recipient (or other authorized individual) is available to immediately retrieve the information to prevent potential review by unauthorized individuals.

Computers/networks/portable devices. NPI documents must be protected during transmission when using computer devices. Only FDA issued computers may be used for processing or storing NPI. Transmission of NPI by

e-mail, Intranet, or Internet is not allowed unless FDA authorized encryption is used.

Permanent Transfer. The only Agency that records can be permanently transferred to is the U.S. National Archives and Records Administration (NARA). The sender shall provide an SF 258, Agreement to Transfer Records to the National Archives of the United States, to the Agency Records Officer (ARO).

Temporary Transfer. Permanent records may be temporarily transferred to the FRC for storage until they are permanently transferred to NARA. The sender shall provide an SF 135, Records Transmittal and Receipt, to the Agency Records Officer.

Temporary Records. Temporary NPI records that are no longer needed on a frequent basis - but should be retained for legal retention until their disposition date - may be transferred to the Federal Records Center for storage.

Reproduction. NPI documents shall be reproduced only as required in the performance of official business. The accountability and safeguarding requirements of reproduced copies shall be the same as that given to the original document(s) from which they were reproduced.

Violations. The loss or misuse of privileged information may seriously hamper FDA in the conduct of its mission. Violations may be punishable by criminal penalties and/or corrective, disciplinary or adverse action. Contractor employees who inappropriately release documents containing NPI may be fined, imprisoned and/or disciplined by action up to and including removal from the Federal service.

Audits. The FDA Privacy and Physical Security Staff may conduct scheduled and unscheduled inspections and/or inventories of NPI document control systems within FDA components and Contractor facilities to ensure effective operation and compliance with this Guide.

Part II - Contract Clauses

Section I, Contract clauses

I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

<https://www.acquisition.gov/far/part-52>

<https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>

FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) CLAUSES:

<u>NUMBER</u>	<u>TITLE</u>	<u>DATE</u>
52.203-3	GRATUITIES	APR 1984
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	JUN 2020
52.203-12	ALTERNATE I (NOV 2021) LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	JUN 2020
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	NOV 2021
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-13	SYSTEM FOR AWARD MANAGEMENT-MAINTENANCE [HHS FAR CD 2025-09, Amendment 2 (Apr. 24, 2026), RFO FAR 4.208(b)(2) (Aug. 14, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS	DEC 2014
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED	(DEVIATION DATE)
52.209-9	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.409 (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)] UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	(DEVIATION DATE)
52.209-10	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.104-7(c) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)] PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	(DEVIATION DATE)
52.212-4	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.108-6(b) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)] TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES, ALTERNATE I	(DEVIATION DATE)
52.219-8	[HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)] UTILIZATION OF SMALL BUSINESS CONCERNS	(DEVIATION DATE)
52.219-27	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 19.109(e)(1) (Feb. 20, 2026), RFO FAR 52 (July 1, 2026)] NOTICE OF SET-ASIDE FOR, OR SOLE-SOURCE AWARD TO,	

Contractor-Hosted Fully Integrated Records Facility (FIRF) IDIQ Recompete
Request for Proposal (RFP) No. 75F40126R00009

	SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB) CONCERNS ELIGIBLE UNDER THE SDVOSB PROGRAM	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 19.106-4(a) (Feb. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-3	CONVICT LABOR	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.201-2 (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1302-2(a)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1401-2(a)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-37	EMPLOYMENT REPORTS ON VETERANS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1302-2(b) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1602-2(a) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-41	SERVICE CONTRACT LABOR STANDARDS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1002-2(b)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-42	STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES	MAY 2014
52.222-43	FAIR LABOR STANDARDS ACT AND SERVICE CONTRACT LABOR STANDARDS-PRICE ADJUSTMENT (MULTIPLE YEAR AND OPTION CONTRACTS)	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1002-2(d)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-50	COMBATING TRAFFICKING IN PERSONS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1703-2(a)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.1802-2 (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-62	PAID SICK LEAVE UNDER EXECUTIVE ORDER 13706	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.2102-5 (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.222-90	ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 22.2203 (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.223-5	POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION	MAY 2024
52.223-23	SUSTAINABLE PRODUCTS	(DEVIATION DATE)
	[HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 23.108(a) (Sept. 30, 2025), RFO FAR 52 (July 1, 2026)]	
52.224-3	PRIVACY TRAINING ALTERNATE I (JAN 2017)	JAN 2017
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.227-1	AUTHORIZATION AND CONSENT	JUN 2020
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	JUN 2020
52.227-14	RIGHTS IN DATA – GENERAL	MAY 2014

Contractor-Hosted Fully Integrated Records Facility (FIRF) IDIQ Recompete
Request for Proposal (RFP) No. 75F40126R00009

52.227-17	RIGHTS IN DATA – SPECIAL WORKS	DEC 2007
52.228-5	INSURANCE – WORK ON A GOVERNMENT INSTALLATION	JAN 1997
52.229-12	TAX ON CERTAIN FOREIGN PROCUREMENTS [HHS FAR CD 2025-06 (Aug. 1, 2025), RFO FAR 29.402-3(b)(1) (July 17, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.232-17	INTEREST	MAY 2014
52.232-23	ASSIGNMENT OF CLAIMS	MAY 2014
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER—SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	MAR 2023
52.233-1	DISPUTES [HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 33.205-9(a) (Aug. 21, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.233-3	PROTEST AFTER AWARD [HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 33.107(b) (Aug. 21, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.233-4	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM [HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 33.205-9(b) (Aug. 21, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.237-1	SITE VISIT	APR 1984
52.237-2	PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION	APR 1984
52.237-3	CONTINUITY OF SERVICES	JAN 1991
52.237-10	IDENTIFICATION OF UNCOMPENSATED OVERTIME	MAR 2015
52.240-91	SECURITY PROHIBITIONS AND EXCLUSIONS [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 40.205(b) (Aug. 14, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.240-93	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 40.303-2 (Aug. 14, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.242-13	BANKRUPTCY	JULY 1995
52.242-15	STOP-WORK ORDER	AUG 1989
52.242-17	GOVERNMENT DELAY OF WORK	APR 1984
52.243-1	CHANGES-FIXED PRICE, ALTERNATE III [HHS FAR CD 2025-05 (Jul. 21, 2025), RFO FAR 43.305(a)(2) (Jun. 12, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.243-3	CHANGES-TIME-AND-MATERIALS OR LABOR-HOURS [HHS FAR CD 2025-05 (Jul. 21, 2025), RFO FAR 43.305(c) (Jun. 12, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.244-6	SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES [HHS FAR CD 2025-11 (Nov. 3, 2025), RFO FAR 44.403 (Sept. 4, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)
52.245-1	GOVERNMENT PROPERTY	SEP 2021
52.245-9	USE AND CHARGES	APR 2012
52.247-34	F.O.B. DESTINATION	JAN 1991
52.247-35	F.O.B. DESTINATION, WITHIN CONSIGNEE’S PREMISES	APR 1984
52.253-1	COMPUTER GENERATED FORMS [HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 53.111 (Sept. 30, 2025), RFO FAR 52 (July 1, 2026)]	(DEVIATION DATE)

I.2 FAR CLAUSES IN FULL TEXT:

FAR 52.216-18 ORDERING (AUG 2020)

- (a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from **the Period of Performance (PoP) start date through 5 years unless extended.**
- (b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.
- (c) A delivery order or task order is considered “issued” when—
- (1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;
 - (2) If sent by fax, the Government transmits the order to the Contractor’s fax number; or
 - (3) If sent electronically, the Government either—
 - (i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or
 - (ii) Distributes the delivery order or task order via email to the Contractor’s email address.
- (d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

FAR 52.216-19 ORDER LIMITATIONS (OCT 1995)

- (a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than **\$10,000.00**, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.
- (b) *Maximum order.* The Contractor is not obligated to honor—
- (1) Any order for a single item in excess of **\$10,000,000.00**;
 - (2) Any order for a combination of items in excess of **\$10,000,000.00**; or
 - (3) A series of orders from the same ordering office within **15 days** that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.
- (c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.
- (d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within **30 days** after issuance, with written notice stating the Contractor’s intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

RFO FAR 52.216-22 INDEFINITE QUANTITY (DEVIATION DATE) [HHSAR FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 16.505(e) (July 1, 2026), RFO FAR 52 (July 1, 2026)]

- (a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
- (b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the “maximum.” The Government shall order at least the quantity of supplies or services designated in the Schedule as the “minimum.”
- (c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
- (d) Any order issued during the ordering period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order, which may include order options to be exercised after the ordering period of this contract but before the end of the period of performance of the order. The contract shall govern the Contractor’s and Government’s rights and obligations with respect to that order, including options exercised, to the same extent as if the order were completed during the contract’s ordering period; provided, that the

Contractor shall not be required to make any deliveries under this contract after 5 years after the expiration of the ordering period of the IDIQ unless the IDIQ contract is extended.

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six (6) months. The Contracting Officer may exercise the option by written notice to the Contractor at any time before the contract expires.

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

- (a) The Government may extend the term of this contract by written notice to the Contractor prior to contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend prior to contract expiration. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years and six (6) months.

RFO FAR 52.219-14 LIMITATIONS ON SUBCONTRACTING (DEVIATION DATE) [HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 19.104-3(c) (Feb. 20, 2026), RFO FAR 52 (July 1, 2026)]

- (a) This clause does not apply to the unrestricted portion of a partial set-aside.
- (b) *Definition. Similarly situated entity*, as used in this clause, means a first-tier subcontractor, including an independent contractor, that—
 - (1) Has the same small business program status as that which qualified the prime contractor for the award (e.g., for a small business set-aside contract, any small business concern, without regard to its socioeconomic status); and
 - (2) Is considered small for the size standard under the North American Industry Classification System (NAICS) code the prime contractor assigned to the subcontract.
- (c) *Applicability*. This clause applies only to—
 - (1) Contracts that have been set aside for any of the small business concerns identified in 19.000(a)(3);
 - (2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);
 - (3) Contracts that have been awarded on a sole-source basis in accordance with sections 19.105, 19.106, 19.107, and 19.108;
 - (4) Orders expected to exceed the simplified acquisition threshold and that are set aside for small business concerns under multiple-award contracts, as described in 8.4 and 16.5;
 - (5) Orders, regardless of dollar value, that are set aside in accordance with sections 19.105, 19.106, 19.107, and 19.108 under multiple-award contracts, as described in 8.4 and 16.5; and
 - (6) Contracts using the HUBZone price evaluation preference to award to a HUBZone small business concern unless the concern waived the evaluation preference.
- (d) *Independent contractors*. An independent contractor shall be considered a subcontractor.
- (e) By submission of an offer and execution of a contract, the Contractor agrees that in performance of a contract assigned a North American Industry Classification System (NAICS) code for—
 - (1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be exceeded. When a contract includes both services and supplies, the 50 percent limitation shall apply only to the service portion of the contract;
 - (2) Supplies (other than procurement from a nonmanufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 50 percent subcontract amount that cannot be

- exceeded. When a contract includes both supplies and services, the 50 percent limitation shall apply only to the supply portion of the contract;
- (3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 85 percent subcontract amount that cannot be exceeded; or
- (4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count towards the prime contractor's 75 percent subcontract amount that cannot be exceeded.
- (f) The Contractor shall comply with the limitations on subcontracting as follows:
- (1) For contracts, in accordance with paragraphs (c)(1), (2), (3) and (6) of this clause—
- ☒ By the end of the base term of the contract and then by the end of each subsequent option period; or
- ☐ By the end of the performance period for each order issued under the contract.
- (2) For orders, in accordance with paragraphs (c)(4) and (5) of this clause, by the end of the performance period for the order.
- (g) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.
- (1) In a joint venture comprised of a small business protégé and its mentor approved by the Small Business Administration, the small business protégé shall perform at least 40 percent of the work performed by the joint venture. Work performed by the small business protégé in the joint venture must be more than administrative functions.
- (2) In an 8(a) joint venture, the 8(a) participant(s) shall perform at least 40 percent of the work performed by the joint venture. Work performed by the 8(a) participants in the joint venture must be more than administrative functions.

(End of clause)

I.3 DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CFR CHAPTER 3) CLAUSES IN FULL TEXT:

HHSAR 352.203-70 ANTI-LOBBYING (JUN 2026) (RFO DEVIATION) [HHSAR CD 2026-11 (Jun. 10, 2026)]

Pursuant to the HHS annual appropriations acts, except for normal and recognized executive-legislative relationships, the Contractor must not use any HHS contract funds for:

- (a) Publicity or propaganda purposes;
- (b) The preparation, distribution, or use of any kit, pamphlet, booklet, publication, electronic communication, radio, television, or video presentation designed to support or defeat the enactment of legislation before the Congress or any State or local legislature or legislative body, except in presentation to the Congress or any state or local legislature itself; or designed to support or defeat any proposed or pending regulation, administrative action, or order issued by the executive branch of any state or local government, except in presentation to the executive branch of any state or local government itself; or
- (c) Payment of salary or expenses of the Contractor, or any agent acting for the Contractor, related to any activity designed to influence the enactment of legislation, appropriations, regulation, administrative action, or Executive order proposed or pending before the Congress or any state government, state legislature or local legislature or legislative body, other than for normal and recognized executive-legislative relationships or participation by an agency or officer of a state, local, or tribal government in policymaking and administrative processes within the executive branch of that government.
- (d) The prohibitions in paragraphs (a), (b), and (c) of this clause include any activity to advocate or promote any proposed, pending, or future federal, state, or local tax increase, or any proposed, pending, or future requirement for, or restriction on, any legal consumer product, including its sale or marketing, including, but not limited to, the

advocacy or promotion of gun control.

(End of clause)

**HHSAR 352.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (FEB 2024)
(DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]**

(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 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 **five (5) business of commencement of work under this 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 Contractor/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 Contractor 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 **10 working 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 **10 working days**.

(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)

HHSAR 352.204-72 RECORDS MANAGEMENT (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

(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.

HHSAR 352.204-73 CONTRACTOR PERSONNEL SECURITY AND AGENCY ACCESS (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

(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 prescreening 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)

**HHSAR 352.204-75 SUPPLY CHAIN RISK ASSESSMENT DURING CONTRACT PERFORMANCE
(OCT 2024) (DEVIATION) [HHSAR CD 2025-01 (Oct. 1, 2024)]**

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

Contract means as defined in FAR 2.101.

Foreign person means as defined in 31 CFR 800.224.

Mission-critical acquisition means the acquisition of products, materials, information, or services that are identified as—

- (1) Contract support or development services for HHS or OpDiv/StaffDiv research and development;
- (2) Contract support or development services for HHS or OpDiv/StaffDiv Financial databases and services;
- (3) Contract support services that require utilization or sharing of HHS or OpDiv/StaffDiv Intellectual property;
- (4) Contract services supporting HHS or OpDiv/StaffDiv continuity of operations (COOP) mission essential functions;
- (5) Contract support services or development initiatives for HHS or OpDiv/StaffDiv critical infrastructure;
- (6) An HHS or OpDiv/StaffDiv high-value/dollar acquisition; or
- (7) Other acquisitions for critical assets or services as identified by OpDiv/StaffDiv leadership.

Office of National Security (ONS) means the HHS office responsible for the management, oversight, policy, guidance, and implementation of the HHS Enterprise Supply Chain Risk Management (E-SCRM) Program, including the conducting of supply chain risk assessments.

State-owned enterprise means a legal entity that is created by a government in order to partake in commercial activities on the government's behalf. A state-owned enterprise or government-owned enterprise is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership.

Supply chain risk means the potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products, materials, information, or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.

Supply chain risk assessment means a systematic examination of supply chain risks, likelihoods of their occurrence, and potential impacts.

Supply chain risk management (SCRM) means a systematic process for managing risk to the integrity, trustworthiness, and authenticity of products, materials, information, and services within the supply chain. It addresses the activities of foreign and other adversaries aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the supply chain. It is conducted through identification of threats, vulnerabilities, and consequences throughout the supply chain and development of mitigation strategies to address the respective risks presented by the supplier, the supplied products, materials, information, and services, or the supply chain at any point during the life cycle.

(b) *Supply chain risk assessment.* The Office of National Security (ONS) or delegated designee may perform a supply chain risk assessment of the Contractor. In performing the supply chain risk assessment, the Government may consider public and non-public information relating to the Contractor's supply chain.

(c) *Updated information and representations.* If requested by the Contracting Officer, or if there are any changes to the information or representations the Contractor has submitted prior to award or during contract performance, the Contractor must submit to the Contracting Officer the information and representations in paragraphs (d) or (e).

(d) *Required information submittal.* The Contractor shall provide the following information for products, materials, information, or services provided during contract performance:

(1) Description of the type of products, materials, information, or services provided.

(2) Vendor and manufacturer's company, if applicable, including name and address.

(3) If known, vendor's and manufacturer's web site, and the Commercial and Government Entity (CAGE)

code and Unique Entity Identifier (UEI).

(e) *Representations.* The Contractor represents that—

(1) It ☐ does, ☐ does not have any foreign ownership, outside of retail shareholders, who control more than 10% of the company's total shares. If yes, identify the legal name of the owning organization/individual and their country of affiliation.

(2) It ☐ does, ☐ does not have any of the following business affiliations with foreign entities: technology development partnerships, strategic partnerships, joint ventures, foreign subsidiaries, grants from a foreign entity. If yes, identify the legal name of the organization, its foreign address, and the nature of the relationship.

(3) It ☐ does, ☐ does not have any foreign governments, or state-owned enterprises that have investments or ownership interest in the company. If yes, identify the foreign government, the ownership stake percentage, and the nature of the relationship.

(4) The company leadership (C-Suite executives, Board members, etc.) ☐ does, ☐ does not have any substantial ties to foreign countries, including being citizens of a foreign country, graduates of a foreign university, or investments in a foreign country. If yes, identify the individual, the nature of the tie, and the country they are tied to.

(5) It ☐ has, ☐ has not violated export controls or the Foreign Corrupt Practices Act within 5 years. If yes, enter the event, the date, and any remediation the company committed after the event.

(6) It ☐ has, ☐ has not been prohibited from doing business with the government of the US or any of its administrative subdivisions to include agencies, states, territories or municipalities. If yes, enter the event, the date, and any remediation the company committed after the event.

(7) It ☐ has, ☐ has not been prohibited from doing business with any foreign governments or subdivisions thereof. If yes, enter the event, the date, and any remediation the company committed after the event.

(8) It ☐ has had, ☐ has not had affiliations with any entities prohibited (e.g. Huawei, see SAM.gov "exclusions" page for additional information regarding prohibited entities) from doing business with the government of the US or any of its administrative subdivisions to include agencies, states, territories or municipalities? If yes, enter the event, the date, and any remediation the company committed after the event.

(9) It ☐ has, ☐ has not been suspended or debarred at any point while doing business with the U.S. Government or any of its administrative subdivisions to include agencies, states, territories or municipalities. If yes, enter the event, the date, and details below.

(10) It ☐ has previously filed for or is currently in, ☐ has not previously filed for or is not currently in bankruptcy in the last 10 years. If yes, enter the event, the date, and details below.

(11) It ☐ was or is currently in, ☐ was not or is not currently in litigation in the last 10 years. If yes, enter the event, the date, and details below.

(f) *Supply chain risk determination.* Findings from the supply chain risk assessment will be considered in connection with a determination of the Contractor's eligibility to continue performance on the contract. The Government reserves the right to limit the disclosure of information to the Offeror regarding the risk in accordance with all applicable laws or regulations.

(g) *Mitigation plans.* Any mitigation plans and amendments determined necessary and to be implemented and sustained during contract performance will be incorporated into the contract.

(h) *Subcontracts.* The Contractor shall include the substance of this clause, including the information and representations in paragraphs (d) and (e), and this paragraph (h), in subcontracts with persons or entities involved the development or delivery of any mission-critical products, materials, information, or services. The Contractor shall

submit all subcontractor information and representations with its proposal for any additional mission-critical products, materials, information, or services during performance of the contract.

(End of clause)

HHSAR 352.208-70 PRINTING AND DUPLICATION (FEB 2026) (RFO DEVIATION) [HHSAR CD 2026-02 (Feb. 7, 2026)]

(a) Unless otherwise specified in this contract, no printing by the Contractor or any subcontractor is authorized under this contract. All printing required must be performed by the Government Printing Office except as authorized by the Contracting Officer. The Contractor must submit camera-ready copies to the Contracting Officer's Representative (COR). The terms "printing" and "duplicating/copying" are defined in the Government Printing and Binding Regulations of the Joint Committee on Printing.

(b) If necessary for performance of the contract, the Contractor may duplicate or copy less than 5,000 production units of only one page, or less than 25,000 production units in aggregate of multiple pages for the use of a department or agency. A production unit is defined as one sheet, size 8.5 x 11 inches, one side only, and one color. The pages may not exceed a maximum image size of 10 3/4 by 14 1/4 inches. This page limit applies to each printing requirement and not for all printing requirements under the entire contract.

(c) Approval for all printing, as well as duplicating/copying in excess of the stated limits, must be obtained from the COR who will consult with the designated publishing services office and provide direction to the contractor. The cost of any unauthorized printing or duplicating/copying under this contract will be considered an unallowable cost for which the Contractor will not be reimbursed.

(End of clause)

HHSAR 352.211-3 PAPERWORK REDUCTION ACT (NOV 2025) (RFO DEVIATION)) [HHSAR CD 2026-01 (Nov. 21, 2025)]

(a) This contract involves a requirement to collect or record information calling either for answers to identical questions from 10 or more persons other than Federal employees, or information from Federal employees which is outside the scope of their employment, for use by the Federal government or disclosure to third parties; therefore, the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) must apply to this contract. No plan, questionnaire, interview guide or other similar device for collecting information (whether repetitive or single time) may be used without the Office of Management and Budget (OMB) first providing clearance. Contractors and the Contracting Officer's Representative must be guided by the provisions of 5 CFR part 1320, Controlling Paperwork Burdens on the Public, and seek the advice of the HHS operating division or Office of the Secretary Reports Clearance Officer to determine the procedures for acquiring OMB clearance.

(b) The Contractor must not expend any funds or begin any data collection until the Contracting Officer provides the Contractor with written notification authorizing the expenditure of funds and the collection of data. The Contractor must allow at least 120 days for OMB clearance. The Contracting Officer will consider excessive delays caused by the Government which arise out of causes beyond the control and without the fault or negligence of the Contractor in accordance with the Excusable Delays or Default clause of this contract.

(End of clause)

HHSAR 352.224-71 CONFIDENTIAL INFORMATION (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

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

Confidential information 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, is identified in this contract.

(c) *Disclosure.* The Contractor shall not disclose confidential information or records until written notice is provided to the Contracting Officer at least 45 days in advance 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.

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

(1) The publication or dissemination of the following types of information are restricted under this contract:

Personally Identifiable Information.

(2) The reason(s) for restricting the types of information identified in subparagraph (d)(1) is/are: **NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).**

(e) The Contractor shall consult with the Contracting Officer when there is uncertainty with regard to the confidentiality of, or a property interest in, information under this contract prior to the release, disclosure, dissemination, or publication of such information.

(End of clause)

HHSAR 352.227-72 PUBLICATIONS AND PUBLICITY (JUN 2026) (RFO DEVIATION) [HHSAR CD 2026-14 (June 30, 2026)]

(a) Unless otherwise specified in this contract, the Contractor may publish the results of its work under this contract. The Contractor must promptly send to the Contracting Officer's Representative—

- (1) A copy of each article submitted for publication;
- (2) Information of when the article or other publication is published; and
- (3) A copy of the published article.

(b) Unless authorized in writing by the Contracting Officer, the Contractor must not display the HHS logo or seal, including Division logos or seals, on any publications.

(c) The Contractor must not reference the product(s) or service(s) awarded under this contract in advertising, as defined in FAR 31.205-1, in any manner which states or implies HHS approval or endorsement of the product(s) or service(s) provided.

(d) The Contractor must include the substance of this clause, including this paragraph (d), in all subcontracts where the subcontractor may propose publishing the results of its work under a subcontract.

(End of clause)

HHSAR 352.231-70 SALARY RATE LIMITATION (FEB 2026) (RFO DEVIATION) [HHSAR CD 2026-02 (Feb. 7, 2026)]

(a) The Contractor must not use contract funds to pay the direct salary of an individual at a rate in excess of the Federal Executive Schedule Level II in effect on the date the funding was obligated.

(b) For purposes of the salary rate limitation, the terms “direct salary,” “salary,” and “institutional base salary,” have the same meaning and are collectively referred to as “direct salary,” in this clause. An individual's direct salary is the annual compensation that the Contractor pays for an individual's direct effort (costs) under the contract. Direct salary excludes any income that an individual may be permitted to earn outside of duties to the Contractor. Direct salary also excludes fringe benefits, overhead, and general and administrative expenses (also referred to as indirect costs or facilities and administrative costs). The salary rate limitation does not restrict the salary that an organization may pay an individual working under a Department of Health and Human Services (HHS) contract or order; it merely limits the portion of that salary that may be paid with contract funds.

(c) The salary rate limitation also applies to individuals under subcontracts.

(d) If this is a multiple-year contract or order, it may be subject to unilateral modification by the Contracting Officer to ensure that an individual is not paid at a rate that exceeds the salary rate limitation provision established in the HHS appropriations act used to fund this contract.

(e) See the salaries and wages pay tables on the Office of Personnel Management web site for Federal Executive Schedule (EX) salary levels at www.opm.gov.

(f) The Contractor must insert the substance of this clause, including this paragraph (f), in all subcontracts.
(End of clause)

**HHSAR 352.239-71 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES
(FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]**

(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)

HHSAR 352.239-74 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

(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)

HHSAR 352.239-75 SECURITY CONTROLS COMPLIANCE TESTING (FEB 2024) (DEVIATION)
[HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

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)

HHSAR 352.239-76 SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED CONTRACTOR-OPERATED AND CONTRACTOR-OWNED CONTRACTOR-OPERATED RESOURCES (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

(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 **within thirty (30) days**. The Contractor must conduct the A&A requirements in accordance with HHS IS2P/FDA IS2P, 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 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) A System Security Plan (SSP) is due **a week prior to the start of the annual security assessment**. 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.

(ii) A Security Assessment Plan/Report (SAP/SAR) is due **before the system is made available to standard users**. The security assessment must be conducted by **FDA's team of security assessors, unless otherwise noted**, 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 and update the SAR at least annually. A copy of the updated SAR shall be provided to the COR, if requested.

(iii) 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.

(iv) 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.

(v) An Independent Assessment is due **before the system is made available to standard users**. 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 before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Actions and Milestones (POA&M).

(vi) The POA&M is due as follows—

(A) Critical-risk weaknesses must be mitigated within **15 calendar days** from the date the weaknesses are formally identified and documented;

(B) High-risk weaknesses must be mitigated within **30 calendar days** from the date the weaknesses are formally identified and documented;

(C) Medium weaknesses must be mitigated within **60 calendar days** from the date the weaknesses are formally identified and documented; and

(D) Low weaknesses must be mitigated within **180 calendar days** 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.

(3) A Contingency Plan and Contingency Plan Test are due **during the annual security assessment**. 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). 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 **annually to facilitate management/oversight efforts.** 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 **monthly.**

(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.

(1) The Contractor also must comply with end of life FDA waiver process.

(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, **FDA Configuration Baselines, FDA Minimum Security Configuration Standards**, and HHS Minimum Security Configuration Standards;
- (3) Maintain the latest operating system patch release and anti-virus software definitions;
- (4) Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
- (5) Automate configuration settings and configuration management in accordance with HHS 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 contact 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)

HHSAR 352.239-77 CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

- (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.
 - (i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at [fedramp.gov](https://www.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 (CONUS).

(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.

(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.

(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. 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: See the A&A package deliverables from paragraph (d)(2) and/or deliverables mentioned in the FedRAMP

Standard Contract Language available on the FedRAMP site. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS and FDA policies using FDA templates.

(iv) Following the initial ATO, the Contractor shall review and maintain the ATO in accordance with HHS policies.

(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. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.
- (vi) The Contractor must comply with FDA POA&M management requirements as specified in the FDA IS2P and FDA POA&M Management Guide, which may impose a more restrictive remediation timeline.

(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 specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

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

- (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 and FDA 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 10 working 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 10 working days.

(i) When the Contractor is responsible for operations or maintenance of the systems, they shall apply security fixes in accordance with the FDA Patch Management Policy (SMG 3210.8) timeframes: critical vulnerabilities within 15 days, high within 30 days, medium within 60 days, and low within 90 days from the date of identification. Emergency or zero-day patches must be applied within 48 hours at the direction of the FDA CISO.

(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).

(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)

HHSAR 352.239-79 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]

(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.

Part III - List of Documents, Exhibits, and Other Attachments

Section J, List of attachments

J.1 LIST OF ATTACHMENTS

The following attachments are provided herein and are incorporated into the solicitation:

- Attachment A: Statement of Work Appendices:
 - Appendix 1: OIMT_IT-Spaces-Cabling-Guidelines
 - Appendix 2: Basic RP LAN Room Layout
 - Appendix 3: FDA Physical Security Requirements
 - Appendix 3A: Addendum to Physical Security Requirements
 - Appendix 4: CDRH Work Functions
 - Appendix 5: FDA-CDRH Document Control Center (DCC) Tracking System Requirements
- Attachment B: Wage Determinations (2015-4269 and 2015-4281)
- Attachment C: IDIQ Pricing Worksheet
- Attachment D: Disclosure of Lobbying Activities SF-LLL
- Attachment E: Sample Task Order Statement of Work
- Attachment F: Labor Category Descriptions
- Attachment G: Past Performance Questionnaire (PPQ)
- Attachment H: Commitment to Protect Non-Public Information (NPI) Employee Agreement Form FDA 3398
- Attachment I: RFP Question Submittal Form
- Attachment J: Contractor Personnel Security Clearance Standards and Residency Requirements (OCT 2017)
- Attachment K: Sample Task Order Pricing Worksheet

Part IV - Representations and Instructions

Section K, Representations, certifications, and other statements of offerors

K.1 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

<https://www.acquisition.gov/far/part-52>

<https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>

FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) PROVISIONS:

<u>NUMBER</u>	<u>TITLE</u>	<u>DATE</u>
52.203-11	CERTIFICATION AND DISCLOSURE REGARDING PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	SEP 2024
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS - REPRESENTATION	JAN 2017
52.209-2	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS-REPRESENTATION	(DEVIATION DATE)
	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.108-6(a) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.209-5	CERTIFICATION REGARDING RESPONSIBILITY MATTERS	(DEVIATION DATE)
	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.104-7(a) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.209-7	INFORMATION REGARDING RESPONSIBILITY MATTERS	(DEVIATION DATE)
	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.104-7(b) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.209-11	REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW	(DEVIATION DATE)
	[HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 9.104-7(d) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]	
52.229-11	TAX ON CERTAIN FOREIGN PROCUREMENTS—NOTICE AND REPRESENTATION	(DEVIATION DATE)
	[HHS FAR CD 2025-06 (Aug. 1, 2025), RFO FAR 29.402-3(a) (July 17, 2025), RFO FAR 52 (July 1, 2026)]	
52.240-90	SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS	(DEVIATION DATE)
	[HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 40.205(a) (Aug. 14, 2025), RFO FAR 52 (July 1, 2026)]	

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in this solicitation. Contracting officers will rely on representations from offers based on provisions in the solicitation. Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

**K.2 DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION
(HHSAR) (48 CFR CHAPTER 3) PROVISIONS IN FULL TEXT:**

HHSAR 352.204-74 SUPPLY CHAIN RISK ASSESSMENT (OCT 2024) (DEVIATION) [HHSAR CD 2025-01 (Oct. 1, 2024)]

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

Contract means as defined in FAR 2.101.

Foreign person means as defined in 31 CFR 800.224.

Mission-critical acquisition means the acquisition of products, materials, information, or services that are identified as—

- (1) Contract support or development services for HHS or OpDiv/StaffDiv research and development;
- (2) Contract support or development services for HHS or OpDiv/StaffDiv financial databases and services;
- (3) Contract support services that require utilization or sharing of HHS or OpDiv/StaffDiv Intellectual property;
- (4) Contract services supporting HHS or OpDiv/StaffDiv continuity of operations (COOP) mission essential functions;
- (5) Contract support services or development initiatives for HHS or OpDiv/StaffDiv critical infrastructure;
- (6) An HHS or OpDiv/StaffDiv high-value/dollar acquisition; or
- (7) Other acquisitions for critical assets or services as identified by OpDiv/StaffDiv leadership.

Office of National Security (ONS) means the HHS office responsible for the management, oversight, policy, guidance, and implementation of the HHS Enterprise Supply Chain Risk Management (E-SCRM) Program, including the conducting of supply chain risk assessments.

State-owned enterprise means a legal entity that is created by a government in order to partake in commercial activities on the government's behalf. A state-owned enterprise or government-owned enterprise is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership.

Supply chain risk means the potential for harm or compromise that arises as a result of security risks from suppliers, their supply chains, and their products, materials, information, or services. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain.

Supply chain risk assessment means a systematic examination of supply chain risks, likelihoods of their occurrence, and potential impacts.

Supply chain risk management (SCRM) means a systematic process for managing risk to the integrity, trustworthiness, and authenticity of products, materials, information, and services within the supply chain. It addresses the activities of foreign and other adversaries aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the supply chain. It is conducted through identification of threats, vulnerabilities, and consequences throughout the supply chain and development of mitigation strategies to address the respective risks presented by the supplier, the supplied products, materials, information, and services, or the supply chain at any point during the life cycle.

(b) *Supply chain risk assessment.* The Office of National Security (ONS) or delegated designee may perform a supply chain risk assessment of the Offeror's proposal. In performing the supply chain risk assessment, the Government may consider public and non-public information relating to the Offeror's supply chain.

(c) *Required information submittal.* The Offeror shall provide the following information for products, materials, information, or services provided under their proposal:

(1) Description of the type of products, materials, information, or services provided.

(2) Vendor and manufacturer's company, if applicable, including name and address.

(3) If known, vendor's and manufacturer's web site, and the Commercial and Government Entity (CAGE) code and Unique Entity Identifier (UEI).

(d) *Representations.* The Offeror represents that—

- (1) It [] does, [] does not have any foreign ownership, outside of retail shareholders, who control more than 10% of the company's total shares. If yes, identify the legal name of the owning organization/individual and their country of affiliation.

(2) It ☐ does, ☐ does not have any of the following business affiliations with foreign entities: technology development partnerships, strategic partnerships, joint ventures, foreign subsidiaries, grants from a foreign entity. If yes, identify the legal name of the organization, its foreign address, and the nature of the relationship.

(3) It ☐ does, ☐ does not have any foreign governments, or state-owned enterprises that have investments or ownership interest in the company. If yes, identify the foreign government, the ownership stake percentage, and the nature of the relationship.

(4) The company leadership (C-Suite executives, Board members, etc.) ☐ does, ☐ does not have any substantial ties to foreign countries, including being citizens of a foreign country, graduates of a foreign university, or investments in a foreign country. If yes, identify the individual, the nature of the tie, and the country they are tied to.

(5) It ☐ has, ☐ has not violated export controls or the Foreign Corrupt Practices Act within 5 years. If yes, enter the event, the date, and any remediation the company committed after the event.

(6) It ☐ has, ☐ has not been prohibited from doing business with the government of the US or any of its administrative subdivisions to include agencies, states, territories or municipalities. If yes, enter the event, the date, and any remediation the company committed after the event.

(7) It ☐ has, ☐ has not been prohibited from doing business with any foreign governments or subdivisions thereof. If yes, enter the event, the date, and any remediation the company committed after the event.

(8) It ☐ has had, ☐ has not had affiliations with any entities prohibited (e.g. Huawei, see SAM.gov “exclusions” page for additional information regarding prohibited entities) from doing business with the government of the US or any of its administrative subdivisions to include agencies, states, territories or municipalities? If yes, enter the event, the date, and any remediation the company committed after the event.

(9) It ☐ has, ☐ has not been suspended or debarred at any point while doing business with the U.S. Government or any of its administrative subdivisions to include agencies, states, territories or municipalities. If yes, enter the event, the date, and details below.

(10) It ☐ has previously filed for or is currently in, ☐ has not previously filed for or is not currently in bankruptcy in the last 10 years. If yes, enter the event, the date, and details below.

(11) It ☐ was or is currently in, ☐ was not or is not currently in litigation in the last 10 years. If yes, enter the event, the date, and details below.

(e) *Supply chain risk determination.* Findings from the supply chain risk assessment will be considered in connection with a determination of the Offeror’s responsibility and eligibility for award. Failure of the Offeror to furnish the information required in this provision or provide additional information as requested by the Contracting Officer may render the Offeror non-responsible and ineligible for award. The Government reserves the right to limit the disclosure of information to the Offeror regarding the risk in accordance with all applicable laws or regulations.

(f) *Mitigation plans.* Any mitigation plans and amendments determined necessary and to be implemented and sustained during contract performance will be incorporated into the contract.

(g) *Subcontracts.* The Offeror shall include the substance of this provision, including the information and representations at paragraphs (c) and (d), and including this paragraph (g), in subcontracts with persons or entities proposed to be used involving the development or delivery of any mission-critical products, materials, information, or services. The Offeror shall submit all potential subcontractor information and representations with its proposal for any mission-critical products, materials, information, or services provided for in the proposal.

(End of provision)

**HHSAR 352.239-72 INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION (FEB 2024)
(DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]**

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)

**HHSAR 352.239-78 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY
NOTICE (FEB 2024) (DEVIATION) [HHSAR CD 2024-01, Amendment 1 (Mar. 1, 2024)]**

(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>.

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.

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.

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/>.

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.

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.

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)

Section L, Instructions, conditions, and notices to offerors or respondents

L.1 SPECIAL INSTRUCTIONS TO OFFERORS ON SUPPLY CHAIN RISK ASSESSMENTS:

As a part of its proposal, the Offeror must submit the completed provision HHSAR 352.204-74, Supply Chain Risk Assessment (Deviation), including all potential subcontractor information and representations as required by paragraph (g) of the provision. See **Section K.2** for the full text of the HHSAR provision.

Supply Chain Risk Assessments

Failure to furnish the required information in HHSAR provision 352.204-74, Supply Chain Risk Assessment (OCT 2024) (DEVIATION), and HHSAR clause 352.204-75, Supply Chain Risk Assessment During Contract Performance (OCT 2024) (DEVIATION), or additional information as requested by the contracting officer may render the—

- (1) Offeror non-responsible and ineligible for award, or
- (2) Contractor ineligible to continue performance on the contract.

L.2 FAR PROVISIONS INCORPORATED BY FULL TEXT:

**RFO FAR 52.204-7 SYSTEM FOR AWARD MANAGEMENT-REGISTRATION (DEVIATION DATE)
[HHS FAR CD 2025-09, Amendment 2 (Apr. 24, 2026), RFO FAR 4.208(b)(1) (Aug. 14, 2025), RFO FAR 52 (July 1, 2026)]**

The Offeror shall have an active Federal Government contracts registration in the System for Award Management (SAM) when submitting an offer or quotation in response to this solicitation and at the time of award. As part of the SAM registration process, the Government collects information, as described in paragraphs (b) through (d) of this provision, that is necessary to identify the Offeror and for the Offeror to be awarded Federal Government contracts. To register in SAM, go to <https://www.sam.gov>. Allow for processing time when registering in SAM. If the Offeror is not registered in SAM, it should register immediately after receiving this solicitation.

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

Commercial and Government Entity (CAGE) code has the meaning provided in the clause at the Federal Acquisition Regulation (FAR) 52.204-13, System for Award Management—Maintenance, of this solicitation.

Electronic Funds Transfer (EFT) indicator means a bank account identifier to establish additional System for Award Management records for identifying alternative EFT accounts (see part 32) for the same entity.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest-level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees. There may be more than one immediate owner (e.g., joint ventures).

Predecessor means an entity whose assets were acquired by the offeror or another entity (most often through merger or acquisition) and whose affairs are now carried out by the offeror or the other entity under a new name.

Taxpayer identification number means the number required by the Internal Revenue Service (IRS) to be used by the offeror to report income tax and other returns. It may be either a Social Security Number or an Employer Identification Number.

Unique entity identifier (UEI) has the meaning provided in the clause at FAR 52.204-13, System for Award Management—Maintenance, of this solicitation.

(b) *Identifiers*. The Offeror shall obtain and provide the following identifying information:

(1) *Unique entity identifier (UEI)*.

(i) The Offeror shall obtain a UEI to register in SAM. The Government will independently validate the existence and uniqueness of the Offeror before assigning a UEI to the Offeror. Go to <https://www.sam.gov> for instructions on obtaining a UEI.

(ii) The Offeror shall enter, in the block with its name and address on the cover page of its offer, the annotation “Unique Entity Identifier” followed by the UEI that identifies the Offeror's name and address exactly as stated in the offer. The Offeror shall also enter its EFT indicator, if applicable.

(iii) The Contracting Officer will use the UEI to verify that the Offeror has an active Federal Government contracts registration in SAM.

(2) *Taxpayer identification number (TIN)*.

(i) The Offeror shall provide its TIN or related information to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d); reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M; and implementing regulations issued by the IRS. The Offeror shall consent for TIN validation; and

(3) *Commercial and Government Entity (CAGE) code*.

(i) The Offeror shall provide a CAGE code and legal business name (Do not use a “doing business as” name) for—

(A) Itself;

(B) Its immediate owner(s), if any;

(C) Its highest-level owner, if any; and

(D) Any predecessor(s), or predecessor of an Offeror's predecessor, that held a Federal contract or grant within the last three years.

(ii) If the Offeror is in the United States or its outlying areas and does not already have a CAGE code assigned, the DLA CAGE Branch will assign a CAGE code to the Offeror as a part of the SAM registration process. For information on obtaining a CAGE code go to <https://cage.dla.mil/>.

(iii) The Offeror shall get from any immediate and/or highest-level owner(s) their respective CAGE code(s) to provide the code(s) as part of the registration (FAR 52.204-7(b)(3)(i)).

(iv) If the Offeror is located outside of the United States or its outlying areas, and does not already have a CAGE code assigned, the Offeror may obtain a CAGE code as indicated in the following table.

Contractor-Hosted Fully Integrated Records Facility (FIRF) IDIQ Recompete
Request for Proposal (RFP) No. 75F40126R00009

If the Offeror is...	Then...
Located in a country that is a member of the North Atlantic Treaty Organization (NATO) or a sponsored nation	Contact the appropriate National Codification Bureau (https://www.nato.int/structur/ac/135/about/contacts)
Located in a country that is not a member of NATO or a sponsored nation	Contact the NATO Support and Procurement Agency (NSPA) (https://eportal.nspa.nato.int/AC135Public/scage/CageList.aspx)

(c) *Representations and certifications.*

(1) The following FAR solicitation provisions contain entity-level representations and certifications that the Offeror shall submit as part of their Federal Government contracts registration in SAM:

Provision	Title	Date
52.204-5	Women-Owned Business (Other Than Small Business)	Oct 2014
52.209-2	Prohibition on Contracting with Inverted Domestic Corporations—Representation	Nov 2015
52.209-5	Certification Regarding Responsibility Matters	Aug 2020
52.209-11	Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law	Feb 2016
52.219-1	Small Business Program Representations	Feb 2024
52.219-1 Alt I	Small Business Program Representations, with its Alternate I	Feb 2024
52.219-1 Alt II	Small Business Program Representations, with its Alternate II	Mar 2023
52.226-2	Historically Black College or University and Minority Institution Representation	Oct 2014

(2) By submitting its offer, the Offeror verifies that, as of the date of its offer, its representations and certifications posted electronically in SAM for the provisions listed in paragraph (c)(1) of this provision are current, accurate, and complete. The Offeror's representations and certifications in SAM are hereby incorporated by reference into its offer.

(d) *Other information.* The Offeror shall provide more information on its business operations and type that is necessary to be considered for award of certain contracts and financial information necessary to receive payment under contracts.

(End of provision)

RFO FAR 52.212-1 INSTRUCTIONS TO OFFERORS – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION DATE) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(a)(1) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]

(a) *Submission of offers.* Submit signed and dated offers to the office specified in this solicitation at or before the exact time specified in this solicitation. As a minimum, offers shall include—

- (1) The solicitation number;
- (2) The name, address, telephone number of the Offeror;
- (3) The Offeror's Unique Entity Identifier (UEI) and, if applicable, Electronic Funds Transfer (EFT) indicator;
- (4) Information necessary to evaluate the factors contained in the provision at 52.212-2 or as described in the solicitation;
- (5) Responses to provisions that require Offeror completion of information, representations, and certifications (other than those collected via the System for Award Management (SAM)); and
- (6) A statement specifying the extent of agreement with all terms, conditions, and provisions included in the solicitation and any solicitation amendments.

(b) *Period for acceptance of offers.* The Offeror agrees to hold the prices in its offer firm for 120 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

(c) *Late submissions, modifications, revisions, and withdrawals of offers.*

- (1) Offerors are responsible for submitting offers and any modifications or revisions to the Government office designated in the solicitation by the time specified in the solicitation.
- (2) Any offer, modification, or revision received after the time specified for receipt of offers is "late" and will not be considered unless it is received before award is made and the Contracting Officer determines that accepting the late offer would not unduly delay the acquisition. However, a late modification of an otherwise successful offer that makes its terms more favorable to the Government will be considered at any time it is received and may be accepted.
- (3) If an emergency or unanticipated event interrupts normal Government processes so that offers cannot be received at the Government office designated for receipt of offers by the exact time specified in the solicitation, and urgent Government requirements preclude amendment of the solicitation or other notice of an extension of the closing date, the time specified for receipt of offers will be deemed to be extended to the same time of day specified in the solicitation on the first work day on which normal Government processes resume.
- (4) Offerors may withdraw their offers by written notice to the Government received at any time before award.

(d) *Contract award (not applicable to Invitation for Bids).* The Government intends to evaluate offers and award a contract without discussions with Offerors. Therefore, the Offeror's initial offer should contain the Offeror's best terms. However, the Government reserves the right to conduct discussions, if necessary. The Government may reject any or all offers if such action is in the public interest, accept other than the lowest offer, and waive informalities and minor irregularities in offers received.

(e) *Debriefings.* If a postaward debriefing is given to requesting Offerors, the Government will disclose the following information, if applicable:

- (1) The agency's evaluation of the significant weak or deficient factors in the debriefed Offeror's offer.
- (2) The overall evaluated cost or price and technical rating of the successful Offeror and the debriefed Offeror and past performance information on the debriefed Offeror.
- (3) The overall ranking of all Offerors when any ranking was developed by the agency during source selection.

(4) A summary of the rationale for award.

(5) For acquisitions of commercial products, the make and model of the product to be delivered by the successful Offeror.

(6) Reasonable responses to relevant questions posed by the debriefed Offeror as to whether the agency followed source-selection procedures set forth in the solicitation, applicable regulations, and other applicable authorities.

(End of provision)

RFO FAR 52.216-1 TYPE OF CONTRACT (DEVIATION DATE) [HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026), RFO FAR 16.105 (July 1, 2026), RFO FAR 52 (July 1, 2026)]

The Government contemplates award of an Indefinite-Delivery, Indefinite-Quantity (IDIQ) type contract resulting from this solicitation.

RFO FAR 52.233-2 SERVICE OF PROTEST (DEVIATION DATE) [HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026), RFO FAR 33.107(a) (Aug. 21, 2025), RFO FAR 52 (July 1, 2026)]

(a) Protests, (as defined in FAR 33.102), that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), must be served on the Contracting Officer identified in the solicitation by obtaining written and dated acknowledgment of receipt from them.

(b) The copy of any protest must be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

L.3 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at these addresses:

- <https://www.acquisition.gov/far/part-52>
- <https://www.acquisition.gov/far-overhaul/far-part-deviation-guide/far-overhaul-part-52>

L.4 PROPOSAL PREPARATION INSTRUCTIONS

Prospective Service-Disabled Veteran-Owned Small Business (SDVOSB) concerns eligible under the SDVOSB program may submit a proposal that will be considered by the Agency. Proposals shall be submitted no later than **2:00 PM Eastern Time, September 21, 2026**. Proposals shall be submitted electronically via email to the Contract Specialist at Melinda.Kim@fda.hhs.gov and the Contracting Officer at Nicholas.Bisher@fda.hhs.gov. The subject line shall read: **RFP 75F40126R00009 FIRF IDIQ Recompete - Proposal**. Late submissions will not be evaluated.

Offerors must submit all questions regarding the RFP to *both* Melinda Kim and Nicholas Bisher, via email, at Melinda.kim@fda.hhs.gov and Nicholas.Bisher@fda.hhs.gov, respectively. The FDA must receive the **questions no later than 2:00 PM Eastern Time, September 10, 2026**. The subject line shall read: **RFP 75F40126R00009 FIRF IDIQ Recompete - Questions**. The FDA may not answer questions received after this date and time and will not answer questions submitted to individuals other than the above-named individuals. **Questions must be submitted using Attachment I: RFP Question Submittal Form**. Questions submitted by another means will not

be answered, including phone calls. The FDA will email, as an amendment, the combined RFP questions and FDA responses to each prospective offeror. It is the vendor's responsibility to confirm receipt of all proposals and/or questions by the closing date of this announcement by contacting the above Contract Specialist/Contracting Officer.

All proposals will be handled in accordance with FAR Subpart 3.104.

The information requested herein shall be furnished in writing and shall be fully and completely in compliance with RFP instructions. The information requested and the manner of submission are essential to permit prompt evaluation of all proposals on a fair and uniform basis. Proposals that do not comply with these instructions will be excluded and not evaluated. Simple statements of compliance without the detailed description of how compliance will be accomplished will not be considered sufficient evidence that the Contractor can meet the technical requirements.

Contractor employees responsible for preparing material that may be proprietary information must mark each page that the Contractor believes contains proprietary information with the legend, "Proprietary Information."

This RFP does not commit the Government to pay any cost for the preparation and submission of a proposal.

General Formatting Instructions

Proposals shall clearly demonstrate an understanding of the Statement of Work (SOW). Any assumptions forming the basis of the submittal shall be clearly identified in the cover letter submitted with the RFP. The Offeror shall submit each part in native format (e.g., Microsoft (MS) Word, Excel, PowerPoint) or as PDF files; however, MS Word/Excel formats are preferred. Failure to provide the required documents in response to this solicitation shall render the Offeror's proposal non-responsive, and the proposal will not be evaluated or considered for award.

The Offeror or applicant shall submit all electronic documents for Microsoft Office suite products without the use of "macros." When submitting proposals via email, DO NOT include .exe, .mso, or any other executable file types that could potentially trigger email security protections (i.e., email blocks, quarantine). **If the Offeror or applicant submits documents that contain macros, macro-referenced files, and/or executable files, the Government will not be able to view or open such documents and the submission will be considered non-responsive to the solicitation.** No additional time will be given to an Offeror or applicant to correct the document submission, and the Government will not inform the Offeror or applicant that their submission is non-responsive prior to award. It is the Offeror's or applicant's responsibility to ensure all electronic documents are submitted without the use of macros.

All text in the proposal shall be single-spaced, and each paragraph shall be separated by at least one (1) blank line. The Offeror is encouraged to use Calibri 11-point font. However, a font of equivalent size may be used. Tables and illustrations may use a reduced font size not less than 9-point and may be landscape. Offerors shall use the following page setup parameters: Page size – 8.5" x 11", Margins (top, bottom, left and right) – 1", Gutter – 0", From edge (header and footer) – 0.5".

To facilitate the award process, ALL proposals shall include a statement in the Cover Letter regarding the terms and conditions herein, as follows:

"The terms and conditions in the solicitation are acceptable to be included in the award document without modification, deletion, or addition."

The signature of an official authorized to bind the Offeror shall be on each proposal.

Each proposal shall consist of a Cover Letter, and three (3) separate volumes (attachments):

- **Cover Letter/Executive Summary (No Page Limitations)**
- **Volumes:**
 - Volume 1 – Technical Proposal (Page Limitation – 75 pages)
 - Volume 2 – Business/Price Proposal (No Page Limitations)
 - Volume 3 – Past Performance (Page Limitation – 20 pages)

The page limitations stated above do not include cover pages, table of contents, dividers, glossary, resumes, CPARS evaluations, or Past Performance Questionnaires.

Incomplete proposals will be considered non-responsive and will not be further evaluated. The cover letter and each

volume **shall be sent as separate attachments**. *The Technical Proposal (Volume 1) and Business/Price Proposal (Volume 2) must be kept separate from each other. “Kept separate” is defined as not including any price information in the Technical Proposal (Volume 1). The Technical Proposal must not make reference to pricing data in order that the technical evaluation may be made strictly on the basis of technical merit. For submission purposes, it is acceptable for Volume 1 and Volume 2 to be submitted in the same email (along with the other required attachments such as the Cover Letter and Volume 3); however, each attachment must be clearly marked as to which Volume it belongs to.*

Note: Attachments must be clearly labeled as to which volume they correspond to.

Each volume shall be submitted as follows:

I. Cover Letter/Executive Summary

- Cover Letter – Shall be signed by an individual that has the authority to bind the company. The cover letter shall include the following, at a minimum:
 - Name of Offeror and Address
 - SAM Unique Entity ID (UEI)
 - Point of Contact – Name, telephone number, and email address
 - Acknowledgement of Latest Amendment – Offerors who fail to acknowledge the most recent amendment may be considered non-responsive
 - Statement that the proposal is valid for 120 calendar days
 - Identification of any teaming arrangements, joint ventures, mentor-protégé relationships, subcontracting relationships, etc.
- As an addendum to the cover letter:
 - Organizational Conflict of Interest (OCI) – The Offeror shall identify any possible OCIs, and if possible OCIs are identified, the Offeror shall submit an OCI mitigation plan. If there is no potential OCI, Offerors must provide a written statement indicating this. If the OCI mitigation plan is deemed unacceptable, the proposal will not be evaluated, and the Offeror will not be eligible for award.
 - Offeror certifications – The Offeror shall certify that **all company information listed in the SAM.gov website is complete, accurate, and current**. Offerors **must** have an active registration in SAM.gov (<https://sam.gov>) with completed representations and certifications, by the close date of the solicitation. Proposals submitted by Offerors not registered in SAM.gov will not be considered.

II. Volume 1 – Technical Proposal

The technical volume is limited to **seventy-five (75)** pages. A page in the technical volume that contains a table, chart, graph, etc., not otherwise excluded below, is subject to the page limitation. Cover pages, table of contents, and resumes are **not** included in the page limit. **Volume 1 shall not make reference to any pricing data.**

General statements that the Offeror can or will comply with the requirements, that standard procedures will be used, that well-known techniques will be used, or paraphrases of the solicitation’s Statement of Work in whole or in part, will not constitute compliance. The following instructions summarize information required to facilitate the Government’s evaluation of each Offeror’s overall technical capabilities.

Technical Factor 1 – Contractor’s Off-Site Facility (One rating will be assigned for this factor)

Offerors must possess, or demonstrate the ability to possess by the time of contract award, a facility that meets the requirements as outlined in the Statement of Work (SOW) and demonstrate that it is capable of meeting all IDIQ Task Area requirements. Offerors must include a detailed blueprint of the proposed facility with their proposals.

The Offeror must provide documentation that the facility demonstrates compliance with all of the following criteria:

- The facility is/will be owned or leased by the Contractor for the entire five (5)-year ordering period of the IDIQ contract and the completion of any resultant task orders (the performance

end date of the last option period of any task order cannot exceed 5 years past the ordering period end date of the IDIQ contract);

- The Contractor must propose ONLY one (1) facility to perform all services during the life of the contract and awarded task orders;
- The facility must be located within a sixty (60)-mile round trip distance from the FDA White Oak Campus, located at 10903 New Hampshire Avenue, Silver Spring, Maryland 20993;
- The facility must be a minimum of 20,000 square feet and be contiguous and capable of supporting the functions described in IDIQ SOW Task Areas. (Refer to **Attachment A: Statement of Work Appendices, Appendix 4: CDRH Work Functions** for current square footage for each Task Order).
- The facility must be capable of having a Verizon data cable line installed for direct connection from the FDA White Oak Campus to the Offeror's facility; and
- A Physical Security Plan that demonstrates the facility meets the Physical Security Requirements/Specifications as outlined in **Attachment A: Statement of Work Appendices, Appendix 3: FDA Physical Security Requirements and Appendix 3A: Addendum to Physical Security Requirements**.

Technical Factor 2 – Technical Understanding and Approach (One rating will be assigned for this factor. Subfactors will not receive individual ratings)

Proposals must detail the Offeror's understanding of the work requirements and describe the Offeror's approach for performing all of the IDIQ task areas. This factor shall address the following technical subfactors:

Technical Subfactor 2.1 – Technical Understanding and Approach to a Sample Task Order

The Offeror shall include a detailed description of its overall technical approach to meeting the requirements of a sample/potential future Task Order (See **Attachment E: Sample Task Order Statement of Work**), while minimizing risk to the FDA. In addition to describing its technical approach, the Offeror shall provide the following:

- A description of any assumptions relied upon in developing the proposed approach.
- A description of how the offeror will achieve at least 95% same-day processing.
- A detailed description of the offeror's tracking system that meets all requirements listed in the FDA/CDRH Document Control Center (DCC) Tracking System Requirements found in **Attachment A: Statement of Work Appendices, Appendix 5: FDA-CDRH Document Control Center (DCC) Tracking System Requirements**.
- A narrative description demonstrating its ability to transition-in (transition-in plan) while ensuring minimal disruption to services, specifically addressing how the offeror will achieve full staff support levels within 90 days of Task Order award.
- A Task Order project management approach/plan that includes the Contractor's Quality Control Plan and describes how the Offeror will monitor performance and ensure quality products and services are delivered.
- A description of the staffing workforce deemed most appropriate for the sample Task Order. Offerors shall propose a staffing mix of IDIQ labor categories in accordance with the labor categories providing in **Attachment K: Sample Task Order Pricing Sheet**, and the staffing plan must address the rationale for personnel choices and describe how and where in the staffing plan they intend to apply them. No pricing information shall be included in the Technical Proposal.

Technical Subfactor 2.2 – Technical Understanding and Approach to the IDIQ

The Offeror shall include a detailed description demonstrating its understanding of, and approach for performing and complying with, all requirements contained in the IDIQ Statement of Work.

Specifically, the proposal must include the following:

- A narrative description of the offeror's approach to performing the task areas described in the IDIQ SOW and how the approach will achieve the objectives identified in the IDIQ SOW. The

narrative must describe the offeror's understanding of the project (from both a business and technical standpoint), how the offeror intends to satisfy the technical requirements, any risks it foresees in the execution of its approach, and mitigation strategies it plans to employ for those risks. The proposal must describe how similar risk and mitigation strategies were executed in similar work under other contracts performed by the offeror.

- A description of the offeror's capability to comply with and accommodate changes in Federal and general legislative mandates and agency policies pertaining to records management (i.e. Federal Records Act per United States Code (U.S.C.), Title 44, Chapters 29 thru 33; Title 36 Code of Federal Regulations (CFR), Chapter 12; MDUFA, 21st Century Cures Act, and National Archives and Records Administration (NARA) guidance).

Technical Factor 3 – Management Approach/Organizational Structure (One rating will be assigned for this factor)

The Offeror must provide a narrative description of its proposed management approach. The description should include contract-level program management and task order management. The description should include a discussion of the IDIQ Program Manager's Role; the proposed organizational structure and how the offeror proposes to manage simultaneous multiple task orders; and staff availability. Staff availability should include a discussion of how the offeror will ensure that qualified resources are available to start performance on the contract, including the necessity of having, or being able to obtain, necessary security clearances. The Offeror should also include a narrative on how it intends to maintain the level of technical qualifications of staff through technology upgrades and staff attrition without increasing the costs to the Government or incurring gaps that are detrimental to the performance of the contract.

The Offeror must submit signed letters of commitment for all key personnel listed in **Section C.8.1**. The letter must be endorsed by the key personnel member to certify that the information provided in their resume is accurate.

A staffing plan that indicates all labor categories expected to be utilized for any task order issued under this IDIQ must be submitted. Additionally, the staffing plan should include the roles and expected contributions of the labor categories of non-key personnel and how the proposed labor categories will be utilized to meet the requirements of the contract and specific task areas. **The staffing plan must NOT include any pricing information.**

The proposal must include resumes and a narrative description of the role(s) of key personnel and the expected level of effort of each individual identified. The narrative should also explain how the Offeror intends to replace key personnel expertise with similar expertise in the event there is attrition, mitigating potential impact on the program. The comprehensive resumes for each proposed key personnel must include current certifications.

If the Offeror intends to or has partnered with another firm, the proposal must clearly describe the division of responsibilities between the firms and the partnership's management structure. If subcontractors will be employed, the proposal must indicate what their roles and responsibilities will be and how they will be managed by the Offeror. If there is a potential conflict of interest, the offeror must submit an acceptable mitigation plan to address such concerns.

All proposed contractor personnel are subject to the security requirements delineated in the FDA Security Article titled, *Contractor Personnel Security Clearance Standards and Residency Requirements*, dated October 2017, as found in **Attachment J**. This includes the requirement pursuant to Homeland Security Presidential Directive-12 (HSPD-12), that proposed personnel must have resided in the U.S. for a total of at least three (3) of the past five (5) years. The offeror must inquire with all proposed personnel to ensure each individual meets such residency requirements prior to submittal of any proposed key personnel, management or staffing plans in response to this solicitation. Thus, any proposal submitted in response to this solicitation will constitute an implied certification that all such residency requirements have been met. The selected offeror is hereby notified that noncompliance with the subject FDA Security Article may detrimentally impact eligibility for award, and remain grounds for cancellation, equitable adjustment, or termination of the contract after award.

Technical Factor 4 –Recent and Relevant Experience (One rating will be assigned for this factor)

The Offeror shall provide a narrative describing up to three (3) prior efforts (i.e., Contract, IDIQ, BPA, Order) that are most like this effort in terms of size, scope, and complexity. The Offeror shall not provide more than three (3) recent and relevant experience references. At least one (1) prior experience shall come from the Offeror who will be the prime contractor for this requirement. “Recent” is defined as active or completed within the last five (5) years. “Relevant” is defined as being of a similar size (i.e., a minimum total contract value of at least \$25,000,000.00), scope (i.e., the successful performance in all of the IDIQ SOW Task Areas), and complexity (i.e., the management of at least one contractor-hosted facility providing similar contractor services for a contract handling the same or higher volume of pre-market and post-market submissions) with the requirements in the SOW. Relevancy is indicated by performing records management work that comprises Records Lifecycle Support, Records Information Management Services, providing high-quality scanned documents, and implementing best practices and improvements to Recordkeeping and Records Management processes. Projects listed may include those entered into with the Federal Government, agencies of state and local Governments, and commercial customers.

Prime/Sub/Teaming Arrangements: The Offeror may use prior experiences in which they served as a prime, subcontractor, and other team organizations. The Offeror must identify the Offeror’s role in all the prior experience submitted. If the Offeror played no role in any submitted prior experience, the Offeror must state that fact. Offerors are encouraged to submit experience performed as a prime, through teaming agreements, or as the sole subcontractor on the relevant projects.

Summary of Data: For any project identified under this **Technical Factor 4**, the offeror must submit the following information:

1. Name of contracting activity (Federal Government agency, local government, commercial customer)
2. Contract Number
3. Contract Type
4. Degree of the offeror’s involvement (prime or subcontractor)
5. Total contract value, and subcontract value (if applicable)
6. Contracting Officer contact information (phone, fax, email)
7. Project Officer/Contracting Officer’s Representative contact information (phone, fax, email)
8. Administrative Contracting Officer contact information – if different from item #6 (phone, fax, email)
9. Description of work
10. Narrative highlighting the relevance of the work performed in terms of size, scope and complexity.
11. These contracts or orders must be in progress or have been completed within the past five (5) years before the proposal date.
12. The list may include contracts/orders under which the Offeror served as a subcontractor, provided that the subcontract was similar in size, scope and complexity to this effort.
13. If a subcontract is being used as relevant experience reference, contact information for the prime contractor, not the customer, must be included.
14. Period of Performance

III. Volume 2 – Business/Price Proposal

Price Factor 6

The offeror shall submit a business proposal fully supported by pricing information adequate to determine the reasonableness of the proposed burdened labor rates and total price. There is no page limitation for the business volume.

Offerors shall propose a fully loaded labor rate for each labor category in **Attachment C: IDIQ Pricing Worksheet** for each 12-month ordering periods, plus the 6-month option period. Offerors are to complete only the yellow highlighted portions of the spreadsheet. No other cells shall be altered in any way or offers may be deemed non-responsive. Offerors shall provide a fully loaded labor rate for all labor categories proposed. Offerors who fail to provide pricing for each labor category and each ordering period may be considered nonresponsive. All pricing shall

be submitted in part in native format (Microsoft (MS) Word, Excel, etc.) or as PDF files, however, MS Word/Excel formats are preferred. The proposed loaded bill rates shall include wages, indirect costs, general and administrative expense and profit. The rates proposed shall serve as the ceiling rates for any given labor category in the resultant IDIQ award.

The offeror's proposal shall indicate whether annual escalation rates are proposed. If escalation is included, the offeror shall state the percent and methodology (e.g., annual flat rate applied to a base rate as of a specific date, or a midpoint rate for the period of performance). Salary increases that are anticipated during contract performance must be claimed under the contract. Plans for any additional compensation resulting from employee relations, profit sharing, pensions or health and welfare benefits must also be included.

The offeror must indicate in its proposal whether it has the necessary financial capacity, working capital, and other resources to perform the contract without assistance from any outside sources (if not, the offeror must indicate the amount required and the anticipated source).

Offerors shall also submit pricing for the sample Task Order by completing **Attachment K: Sample Task Order Pricing Worksheet**. Prices proposed for the sample Task Order must be in accordance with the base IDIQ prices quoted in the offeror's submission for **Attachment C: IDIQ Pricing Worksheet**. Offerors are to complete only the yellow highlighted portions of the spreadsheet. No other cells shall be altered in any way or offers may be deemed non-responsive.

Additional Documents to be Submitted with the Business Proposal:

1. Completed Pricing Worksheet (**Attachment C: IDIQ Pricing Worksheet**) for the IDIQ
2. Completed Pricing Worksheet (**Attachment K: Sample Task Order Pricing Worksheet**) for the sample Task Order
3. Disclosure and Use of Lobbying Activities: If the offeror has any activity to report, the offeror shall complete **Attachment D: Disclosure of Lobbying Activities SF-LLL** and shall include one (1) originally signed copy with the business proposal.

IV. Volume 3 – Past Performance

Past Performance Factor 5

Volume 3 shall include a listing of the projects and the points of contact for which a Past Performance Questionnaire (PPQ) was sent. The Offeror shall send the Past Performance Questionnaire (PPQ) attached to this solicitation as **Attachment G** to the references for each of the projects that it identifies in its response to **Technical Factor 4 –Recent and Relevant Experience**. The questionnaires must be sent to the individuals most knowledgeable about the offeror's performance on the identified order or program (e.g., the Contracting Officer's Representative, the Program/Project Manager, or the Contracting Officer). Each reference must complete the questionnaire and email an electronic copy to the Contract Specialist and Contracting Officer by no later than the proposal due date. The offeror shall ensure that all the points of contact complete and return the questionnaires to the Government electronically prior to the solicitation close date, to the Contract Specialist, Melinda Kim, at Melinda.Kim@fda.hhs.gov, and to the Contracting Officer, Nicholas Bisher, at Nicholas.Bisher@fda.hhs.gov, with the subject reference "**RFP 75F40126R00009 FIRF IDIQ Recompete - PPQ**". CPARS reports may be submitted by the Offeror in lieu of PPQs; however, the CPARS reports must provide a detailed description of the services provided and provide ratings and detailed justifications for those ratings.

Offerors are cautioned that the Government may use data provided by each offeror as well as data obtained from possible other sources, such as Government past performance databases (i.e., Past Performance Information Retrieval System (PPIRS), CPARS) in the evaluation of past performance. Offerors are urged to verify accuracy of all data provided. Past Performance information regarding predecessor companies, key personnel who have relevant experience, and subcontractors that will perform major or critical aspects of the requirement may be provided as past performance submissions. The Government is not responsible for ensuring that a sufficient number of questionnaires are submitted.

The Government reserves the right to consider questionnaires received after the due date of the solicitation. The Government reserves the right to contact references for verification or additional information, and the right to consider other relevant past performance information. The Government may call customers, whether or not listed on the provided list, to inquire about the offeror's past performance. The Government does not assume the duty to search for data to cure the problems it finds in the information provided by the offeror. The burden of providing thorough and/or complete past performance information remains with the offeror.

Section M, Evaluation factors for award

**M.1 PROSPECTIVE CONTRACTOR RESPONSIBILITY AND ELIGIBILITY STANDARDS:
SUPPLY CHAIN RISK ASSESSMENT**

The standards and procedures for determining prospective contractor and subcontractor responsibility will be in accordance with RFO FAR Subpart 9.1, Responsible Prospective Contractors (Apr. 20, 2026) [adopted via HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026)].

Special standards in the responsibility determination: The Government will assess the Offeror's submitted information in provision HHSAR 352.204-74, Supply Chain Risk Assessment (Deviation), any required supporting data, and information from other sources for the purpose of evaluating foreign ownership, control or influence and other areas of supply chain risk, when necessary, and this information will be treated by HHS, to the extent permitted by law, as business or financial information submitted in confidence.

In accordance with RFO FAR 15.202(a)(2)(iii) (Sept. 30, 2025) [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)], the Government may request additional information or a mitigation plan from the Offeror that addresses risks identified in the supply chain risk assessment.

Any mitigation plans and amendments determined necessary and required to be implemented and sustained during contract performance will be incorporated into the contract.

In order to manage supply chain risk, the Government may consider information, public and non-public, relating to an Offeror's supply chain in determining responsibility. The Government may remove the Offeror from further consideration due to a Supply Chain Risk determination, which renders the offeror nonresponsible. The Government reserves the right to limit the disclosure of information to the Offeror regarding the risk in accordance with all applicable laws or regulations.

Failure by the Offeror to affirmatively demonstrate adequate compliance with the general standards of prospective contractor responsibility set forth at RFO FAR 9.104-1 may result in a determination of nonresponsibility. As with all aspects of prospective contractor responsibility, a finding of nonresponsibility can be made at any time prior to contract award. In accordance with RFO FAR 9.103(b), if the prospective contractor is a small business concern, the Government must comply with the procedures set forth at RFO FAR Subpart 19.204, Certificate of Competency (Feb. 20, 2026) [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)].

M.2 FAR PROVISIONS INCORPORATED BY FULL TEXT:

RFO FAR 52.212-2 EVALUATION – COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (DEVIATION DATE) [HHS FAR CD 2025-09, Amendment 1 (Nov. 3, 2025), RFO FAR 12.205(a)(2) (Apr. 20, 2026), RFO FAR 52 (July 1, 2026)]

(a) *Evaluation factors.* The Government will award a contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The Government will evaluate competitive offers using the lowest price technically acceptable (LPTA) approach to source selection. The following factors will be used to evaluate offers:

- **Technical Factor 1 – Contractor's Off-Site Facility (One total rating)**
- **Technical Factor 2 – Technical Understanding and Approach (One total rating)**
 - **Technical Subfactor 2.1 – Technical Understanding and Approach to a Sample Task Order**
 - **Technical Subfactor 2.2 – Technical Understanding and Approach to the IDIQ**
- **Technical Factor 3 – Management Approach/Organizational Structure (One total rating)**
- **Technical Factor 4 –Recent and Relevant Experience (One total rating)**
- **Past Performance Factor 5**
- **Price Factor 6**

(b) *Options*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. The evaluation of options does not obligate the Government to exercise the option(s).

(c) *Notice of award*. A written notice of award or acceptance of an offer furnished to the successful Offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

RFO FAR 52.217-5 EVALUATION OF OPTIONS (DEVIATION DATE) [HHS FAR CD 2025-12 (Nov. 3, 2025), RFO FAR 17.203(c) (Sept. 11, 2025), RFO FAR 52 (July 1, 2026)]

Except when it is determined in accordance with FAR 17.202(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

(End of provision)

M.3 BASIS FOR AWARD

Award will be made to the lowest-priced offeror whose proposal is determined to be technically acceptable for all factors and whose past performance is assessed as technically acceptable. Technical Factors 1–4 and Past Performance will be evaluated on an acceptable/unacceptable basis. No trade-offs will be made between technical merit, past performance, and price. There will be only one rating per factor. Subfactors will not receive individual ratings.

The Government intends to award one (1) contract resulting from this solicitation to the responsible SDVOSB concern whose proposal, conforming to the Request for Proposal, represents the best value to the Government—price and other factors considered. Best value will be determined using the LPTA process. The Government reserves the right to award without conducting post-proposal exchanges with Offerors. Therefore, the Offeror's initial proposal should contain the Offeror's best terms from a price and technical standpoint. However, the Government may conduct post-proposal exchanges if the Contracting Officer determines they are necessary. To be eligible for an award, the Offeror must be determined responsible in accordance with the standards in RFO FAR Subpart 9.1, Responsible Prospective Contractors (Apr. 20, 2026) [adopted via HHS FAR CD 2025-10, Amendment 1 (Apr. 24, 2026)].

The award of the resultant contract will be based upon a review of all proposals against the following evaluation factors:

- Technical Factor 1 – Contractor's Off-Site Facility
- Technical Factor 2 – Technical Understanding and Approach
 - Technical Subfactor 2.1 – Technical Understanding and Approach to a Sample Task Order
 - Technical Subfactor 2.2 – Technical Understanding and Approach to the IDIQ
- Technical Factor 3 – Management Approach/Organizational Structure
- Technical Factor 4 –Recent and Relevant Experience
- Past Performance Factor 5
- Price Factor 6

The Government reserves the right to make a competitive award without negotiations in accordance with RFO FAR 15.203 (Sept. 30, 2025) [adopted via HHS FAR CD 2026-01, Amendment 2 (Apr. 24, 2026)].

M.4 EVALUATION CRITERIA

Technical Factor 1 – Contractor's Off-Site Facility

The Government will evaluate proposals on an Acceptable/Unacceptable basis to determine whether the Offeror's proposed facility meets all required criteria described below. To be eligible for award, the Offeror's proposed facility must meet the following criteria:

- The facility must be owned or leased by the Offeror, or the proposal must demonstrate that the facility will be owned or leased by the Offeror by the time of contract award.
- Only one (1) facility is proposed to perform all services during the life of the IDIQ contract and awarded task orders.
- The facility must be located no more than sixty (60) miles, round trip, in distance from the FDA White Oak Campus, located at 10903 New Hampshire Avenue, Silver Spring, Maryland.
- The proposed facility must be a minimum of 20,000 square feet and be contiguous and capable of supporting the functions described in the IDIQ SOW Task Areas. (Refer to **Attachment A: Statement of Work Appendices, Appendix 4: CDRH Work Functions** for current square footage for each TO).
- The facility must be capable of having a Verizon data cable line installed for direct connection from the FDA White Oak Campus to the Offeror's facility.
- The facility's Physical Security Plan shall demonstrate that the proposed facility meets the Physical Security Requirements/Specifications as outlined in **Attachment A: Statement of Work Appendices, Appendix 3: FDA Physical Security Requirements and Appendix 3A: Addendum to Physical Security Requirements**.

A proposal that fails to meet any one of the above criteria will be rated **Unacceptable** and will not be considered for award.

Technical Factor 2 – Technical Understanding and Approach (Only one total rating will be assigned for this factor, including all subfactors)

The Government will evaluate proposals under this factor on an Acceptable/Unacceptable basis.

Technical Subfactor 2.1: Technical Understanding and Approach to Sample Task Order

A proposal will be rated **Acceptable** if it fulfills the following objective criteria:

- Demonstrates a complete understanding of all the sample Task Order requirements and presents a sound approach to satisfying those requirements. (See **Attachment E: Sample Task Order Statement of Work**).
- Demonstrates the ability to achieve at least 95% same-day processing
- Demonstrates that the offeror has a tracking system that meets all requirements listed in the FDA/CDRH Document Control Center (DCC) Tracking System Requirements found in **Attachment A: Statement of Work Appendices, Appendix 5: FDA-CDRH Document Control Center (DCC) Tracking System Requirements**.
- Demonstrates that the offeror understands any project risks and can take steps to mitigate those risks.
- Details activities that should result in successful completion of the requested work, including an adequate transition-in plan (if applicable).
- Details task order project management approach/plan that includes the Contractor's Quality Control Plan and describes how the Offeror will monitor performance and ensure quality products and services are delivered.
- Proposes staff that have the required skills and expertise for a project of this magnitude in accordance with the requirements in **Attachment F: Labor Category Descriptions**.

Note: sample/potential future Task Order is for evaluation purposes only.

Technical Subfactor 2.2: Technical Understanding and Approach to the IDIQ

A proposal will be rated **Acceptable** if it fulfills the following objective criteria:

- Demonstrates an understanding of the Task Areas set forth in the IDIQ SOW; its approach

satisfies the complete range of technical requirements in a manner that is technically sound, logical, and likely to be effective in achieving the IDIQ SOW and demonstrates an understanding of the mitigation strategies for potential risks.

- Demonstrates its capability to comply with, and accommodate changes in, Federal legislative mandates and agency policies pertaining to records management.

A proposal that fails to meet any of the objective requirements above for **the subfactor** will be rated **Unacceptable, as only one total rating will be applied to this factor.**

Technical Factor 3 – Management Approach/Organizational Structure

The Government will evaluate proposals under this factor on an Acceptable/Unacceptable basis. A proposal will be rated **Acceptable** if it fulfills the following objective criteria:

- Demonstrates a comprehensive and effective management approach and organizational structure to ensure the accomplishment of FDA's requirements.
- Demonstrates the ability to manage all aspects of contract performance and ensure high-quality services and deliverables.
- Demonstrates a workforce management approach, staffing plan, and Subcontractor/Teaming Management approach that show clear lines of authority (also between the prime and subcontractor, if applicable), present a resourcing and retention approach that is logical and technically effective, and satisfy the requirements of the IDIQ SOW.
- Includes signed letters of commitment for all key personnel listed in **Section C.8.1 of this solicitation.**

A proposal that fails to address or include any of the objective criteria listed above will be rated **Unacceptable.**

Technical Factor 4 – Recent and Relevant Experience

The Government will evaluate proposals under this factor on an Acceptable/Unacceptable basis. A proposal will be rated **Acceptable** if it provides a minimum of two (2) experience references for contracts/orders/BPAs that are active or completed within the past five (5) years.

At least two (2) references must meet the following objective criteria:

- **Comparable Size:** Features a minimum total contract value of at least \$25,000,000.00.
- **Comparable Scope:** Demonstrates successful performance in all of the IDIQ SOW Task Areas.
- **Comparable Complexity:** Required the management of at least one contractor-hosted facility providing similar contractor services for a contract handling the same or higher volume of pre-market and post-market submissions.

A proposal that fails to provide the required number of references meeting all the metrics above will be rated **Unacceptable.**

Past Performance Factor 5

(a) **Evaluation Method:** Past performance will be evaluated on an Acceptable or Unacceptable basis. A comparative assessment of past performance information will not be conducted. The Government will review recent and relevant past performance information to determine the Offeror's capability to successfully execute the IDIQ SOW requirements based on its historical performance record.

(b) **Definitions:**

- **Acceptable:** Based on the Offeror's performance record, the Government has a reasonable expectation that the Offeror will successfully perform the required effort. This rating is assigned to offerors whose references demonstrate satisfactory or higher performance in meeting contract specifications, schedules, and quality standards on projects of similar size and scope.
- **Unacceptable:** Based on the Offeror's performance record, the Government does not have a reasonable expectation that the Offeror will successfully perform the required effort. This rating is assigned if the historical record shows significant or systemic performance deficiencies, unresolved cure notices, unsatisfactory CPARS ratings, or repetitive failures to adhere to contract schedules and quality metrics.

- **Neutral:** will be treated as Acceptable.

(c) **Information Sources:** The Government will consider information provided by the offeror, as well as information obtained from any other sources. The Government will evaluate past performance questionnaires (PPQs) submitted with the proposal. The Government also reserves the right to obtain and utilize past performance data from independent sources, including the Contractor Performance Assessment Reporting System (CPARS), Federal databases, or interviews with prior Program Managers.

(d) **Considerations:** The Government will consider any information regarding predecessor companies, key personnel who have relevant experience, or subcontractors that will perform major or critical aspects of the requirement when such information is relevant to the instant acquisition.

(e) **Joint Ventures:** The Government will consider the past performance of the joint venture, when evaluating an offer from a joint venture. If the joint venture does not demonstrate past performance for award, the past performance of each party to the joint venture must be considered.

(f) **No Past Performance Information:** An offeror without a record of relevant past performance or for whom information on past performance is not available will not be evaluated favorably or unfavorably on past performance. An offeror without a record of recent or relevant past performance will be assigned a Neutral rating, which will be treated as "Acceptable".

(g) **Clarifications:** The Government reserves the right to conduct clarifications with an offeror to address the relevance of an offeror's past performance information and adverse past performance information to which the offeror has not previously had an opportunity to respond. Clarifications may occur, at the Contracting Officer's discretion, at any time after receipt of proposals through contract award. Contracting Officers are not required to conduct clarifications with an offeror. If the Contracting Officer conducts clarifications with one or more offerors, it is not required to conduct clarifications with any other offeror.

Please note that the past performance experiences must come from those identified in the Offeror's response to Technical Factor 4 – Recent and Relevant Experience.

Price Factor 6

Evaluation Method: The Government will evaluate proposals by performing price analysis.

IDIQ Pricing Constraints: The proposed fully burdened labor rates will serve as the maximum ceiling rates for any resultant task order awarded under the IDIQ. The successful Offeror's Total Evaluated Price is used for evaluation purposes only and will not be incorporated as a contract ceiling. The Government will assign a contract ceiling at award.

Completeness: A proposal will be deemed incomplete and may be rejected if the Offeror fails to provide a price for every required labor category, changes the level of effort required for a labor category, or provides pricing that includes incorrect math / computation.