i. This is a combined synopsis/solicitation for commercial products or services prepared in accordance with the Federal Acquisition Regulation (FAR) format in Subpart 12.6, as supplemented with additional information included in this notice.. This announcement constitutes the only solicitation; a written solicitation will not be issued.

Offerors must have an active registration in SAM.gov when submitting a proposal and at time of award in order to comply with the annual representations and certifications requirements. Proposals submitted by Offerors without an active registration in SAM.gov or without completed representations and certifications by the close date of the solicitation may not be considered.

The FDA is not responsible for any costs incurred in preparing the documents described in this RFP. Offeror employees responsible for preparing material that may be proprietary information must mark each page that the Offeror believes contains proprietary information with the legend "Proprietary Information."

ii. The solicitation number is 75F40126R00042. The solicitation is issued as a Request For Proposal (RFP).

iii. The solicitation document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular (FAC) 2026-01, effective March 13, 2026, and the Revolutionary Federal Acquisition Regulation Overhaul, effective April 17, 2026.

iv. This requirement is being solicited as a **competitive 8(a) set-aside**; only those companies certified by the U.S. Small Business Administration as an 8(a) business that have not graduated from the program are eligible for award. The associated North American Industry Classification System (NAICS) Code is *541519 Other Computer Related Services* ; Small Business Size Standard is $34 million.

v. The US Food & Drug Administration (FDA) intends to issue a Commercial Item Firm Fixed-Price/Labor Hour single-award Indefinite-Delivery Indefinite-Quantity (IDIQ) contract that represents the best value to the Government, technical, price and other factors considered, in accordance with the evaluation criteria set forth in this solicitation. Please submit all proposals with:
a) Pricing for all line items

CLIN	Description	Anticipated POP
1	Ordering Period 1: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2026 – 09/28/2027
2	Ordering Period 2: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2027 – 09/28/2028
3	Ordering Period 3: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2028 – 09/28/2029
4	Ordering Period 4: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2029 – 09/28/2030
5	Ordering Period 5: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2030 – 09/28/2031

6	52.217-8 – 6mo Extension: Food Applications Regulatory Management (FARM) & IT Interfacing Systems	09/29/2031 – 03/28/2032

*Proposals that do not price all line items may be deemed *non-responsive*.

vi. and vii. **Description of Requirement and Attachments**

a. Attachment_1_IDIQ_SOW – Description of Requirement
b. Attachment_2_TO1_SOW_OM
c. Attachment_A_Pricing Schedule and LCAT
d. Attachment_B_Appendix_I

viii. The provision at **52.212-1, Instructions to Offerors-Commercial Products and Commercial Services**, applies to this acquisition. Additional instructions are detailed below.

This section provides instructions for preparing proposals for the solicitation. Offeror's are cautioned to follow the instructions carefully to assure the Government receives consistent information in a form that will facilitate proposal evaluation. For the purposes of preparing proposals, offeror's should assume an award timeframe of August 2026.

The Government intends to conduct this procurement through a phased proposal submission process with written submissions using an evaluation process.

a. Instructions for Proposal Preparation

Offerors are instructed to read the entire RFP document, including all attachments, prior to submitting questions and/or preparing your proposal. Omission of any information from the proposal submission requirements may result in rejection of the proposal.

Offerors shall note that proposals will be evaluated, and a selection decision will be made. Offers are expected to follow the detailed proposal preparation instructions fully and carefully. The Government will rely on the information provided by the Offerors to evaluate the proposals. It is therefore imperative that Offerors carefully follow the instructions set forth below and submit their proposals in the format and with the content specified below, providing all requested information.

The Offerors are responsible for the accuracy and completeness of their proposal. Please note: this IDIQ is being solicited concurrently with the Task Order 1. By responding to the solicitation, Offerors acknowledge the proposal's validity through **December 31, 2026**.

b. Page Size and Font

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 electronically submitted PDF document 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. The Offeror 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".

It is the sole responsibility of the Offeror to ensure that the electronic media submitted is virus-free and can be opened and read by the Government. The deadline for submission of the electronic copy of the proposal is firm. As the closing date and time draws near, heavy traffic on the web server may cause delays. Offeror's are strongly encouraged to plan and leave ample time to prepare and submit their proposal. Offeror's bear the risk of web site inaccessibility due to heavy usage, which may occur during the final days/hours before the RFQ closing time. The electronic copy of the proposal will constitute the official copy for timely receipt.

c. Proposal Content

The CS, identified in Section XIV is the main point of contact for this acquisition. The required elements of proposal submission are provided in Table 1 below. The Cover Letter and Resumes will be in PDF format and the Pricing Worksheet will be in excel format.

d. Advisory Down-Selection Notification

After the Government completes the evaluation of Phase I, Offerors will receive an advisory notification via e-mail from the Government. This notification will advise the Offeror of the Government's advisory recommendation to proceed or not to proceed with Phase II submission. Offerors who are rated most highly in Phase I will be advised to proceed to Phase II of the proposal submission process. Offerors who were not among the most highly rated will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advice is to minimize proposal development costs for those Offerors with little to no chance of receiving an award.

The Government will determine the appropriate number of Offerors for Phase II that is most beneficial to the Government. However, the Government's advice will be a recommendation only, and those Offerors who are advised not to proceed may elect to continue their participation in the procurement.

Failure to participate in Phase I of the procurement precludes further consideration of an Offeror. Phase II submissions will not be accepted from Offerors who have not submitted Phase I proposals by the due date and time stated in this solicitation. For those Offerors that are highly rated and advised to proceed to Phase II of the proposal submission process, the CO/CS will include the date and time for submissions. The Government recommends Offerors begin

preparation of Phase II proposals only after receipt of the Phase I advisory down-select notice.

Table 1.

Naming Convention	Tab Title
Volume I: Relevant Experience (Phase I)	
Tab A (Document)	Relevant Experience Criteria (6-page limit)
Tab B (Document)	Offeror Information and Confirmation
Volume II: IDIQ Technical Proposal (Phase II) (50-Page Limit)	
Tab A (Document)	IDIQ Overall Understanding & Approach
TAB B (Document)	Approach to Task Order (TO) #1 – Operations & Maintenance (O&M)
TAB C (Document)	Management Approach
Volume III: Business & Pricing	
Tab A (Document)	Proposal Cover/Transmittal Letter
Tab B (Document)	Pricing Excel Workbook (Attachment A)
Tab C (Document)	Proposal Assumptions, Exceptions, and Dependencies

- Information contained in each volume shall be complete to the extent that evaluation of each tab may be accomplished independently of, and concurrently with, evaluation of the others. Your responses must demonstrate that both your firm and personnel can successfully complete this project. Offerors shall strictly adhere to the page limits.

- NO PRICE INFORMATION IS TO BE INCLUDED IN VOLUME I or VOLUME II

e. Solicitation Questions & Comments

Questions/clarifications regarding this requirement shall be submitted via email to the Contract Specialist, Brian Wodzisz at Brian.Wodzisz@fda.hhs.gov, and the Contracting Officer, Peter Lee at Peter.Lee@fda.hhs.gov, **by 3:00pm (Eastern) on August 7th, 2026.** FDA may not answer questions received after this date and time and may not answer questions submitted to individuals other than the named contacts. Questions submitted by another means may not be answered, including phone calls. It is the Offeror'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. It is the Offeror's responsibility to exercise due diligence to discover and bring to the attention of the CS and CO at the earliest possible time, any ambiguities, discrepancies, inconsistencies, or conflicts between the statement of work (SOW) and other documents attached hereto or incorporated by reference herein.

ix. The provision at **52.212-2, Evaluation-Commercial Products and Commercial Services (NOV 2025)** is **not** applicable to this requirement. The specific procedures are detailed below.

a. Basis of Award

The Government intends to award an IDIQ from this solicitation to the responsible offeror whose proposal represents the best value to the Government, technical, price and other factors

considered. There is one (1) Task Order (TO) Statement of Work (SOW) which the government reserves the right to award at time of the Base IDIQ award.

The Request for Proposal (RFP) shall not be considered direction to proceed with the subject effort, nor a promise of future direction to process.

The following factors shall be used to evaluate proposals:

- Factor 1: Relevant Experience Criteria (Phase I)
- Factor 2: IDIQ Overall Understanding & Approach (Phase II)
    - Subfactor 1: Approach to Task Order (TO) #1 (Operations & Maintenance (O&M)) (Phase II)
- Factor 3: Management Approach (Phase II)

Non-price factors combined are significantly more important than price. As technical merit of proposals becomes equal, the evaluated price may become the determining factor.

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

b. Evaluation Factors & Criteria

VOLUME I: RELEVANT EXPERIENCE CRITERIA SUBMISSION INSTRUCTIONS & EVALUATION (6-page limit) (PHASE I)

TAB A: Factor 1: Relevant Experience Criteria
Instructions: The Offeror shall provide a written narrative describing at least three (3) Government experiences (Federal, State, and Local, Commercial Customers) that are like this effort in terms of type, scope, complexity, technology, and size. The proposed projects that are included in the narrative should involve experience in implementations and other work related to the task areas described in the Statement of Work. **At least one (1) project shall demonstrate experience relevant to Operations and Maintenance (O&M) activities, and at least one (1) project shall demonstrate experience relevant to Development, Modernization, and Enhancement (DME) activities.** At least **one (1) project** must also involve Artificial Intelligence applications to enhance the findability of relevant records or information from various IT systems **or to automate regulatory review processes, document processing, or decision support capabilities**.

For projects demonstrating O&M experience, the narrative should highlight:

- 24/7 system operations and monitoring for mission-critical systems
- Database administration and performance tuning
- Release management and testing support
- Multi-tier user support/helpdesk operations
- Collaboration with data center and cloud environment providers

- IT system consolidation and modernization support

For projects demonstrating DME experience, the narrative should highlight:

- AI/ML implementation in regulatory or enterprise systems
- Workflow automation and optimization using platforms such as Appian
- System integration across multiple platforms and data sources
- Development of intelligent document processing capabilities
- Implementation of information findability across disparate repositories through integration with enterprise search capabilities, enabling multi-source query federation to retrieve and surface relevant content from multiple systems simultaneously.
- Cloud-based application development and deployment"

Projects listed may involve contracts with the Federal Government, Agencies of States and Local Governments, or commercial customers.

The terms scope, complexity, and size, are defined below:

- **Scope**: is defined as relevant experience that are the same or similar to the Attachment_1_IDIQ_SOW requirements and task areas in Attachment_1_IDIQ_SOW.
- **Complexity**: Complexity is defined as the number of helpdesk ticket requests from internal or external system users and number of change requests handled by the offerors. The anticipated number of requests is at least eight hundred (800) annually.
- **Technology**: Please refer to the technology mix under Attachment_1_IDIQ_SOW - Table 2. Current System technology stack
- **Size**: is defined as the total dollar contract value, at least one relevant experience is required to have a minimum dollar value $1,000,000.00 in which they were the Prime contractor.

The Offeror's shall, for each relevant experience contract identified above, submit the following information (if a subcontract, contact information for the prime contractor, not the customer, shall be included):

1. Name of contracting activity (Federal Government agency, State/local government, commercial customer);
2. Name of company who performed the work;
3. Contract number;
4. Contract type;
5. Total contract value, and subcontract value (if applicable); -or-
6. If an order, the total value of just the order for which the Offeror was awarded;
7. Contracting Officer contact information (name, phone number, email);
8. Brief Description of scope and technical requirements;
9. Relevance to this requirement;
10. Period of performance of the project.

Evaluation: The government will assess its level of confidence that the Offeror's relevant experience submissions demonstrate performance on current and/or previous contracts that are relevant to the Statement of Work in terms of type, scope, complexity, technology, and size.

The Offeror's shall, for each relevant experience contract identified above, submit the following information (if a subcontract, contact information for the prime contractor, not the customer, shall be included):

1. Name of contracting activity (Federal Government agency, State/local government, commercial customer);
2. Name of company who performed the work;
3. Contract number;
4. Contract type;
5. Total contract value, and subcontract value (if applicable); -or-
6. If an order, the total value of just the order for which the Offeror was awarded;
7. Contracting Officer contact information (name, phone number, email);
8. Brief Description of scope and technical requirements;
9. Relevance to this requirement;
10. Period of performance of the project.

TAB B: Offeror Information and Confirmation
Instructions: The Offeror shall provide the following information:

a. Reference to RFP #75F40126R00042
b. Company name; address; SAM UEI; Cage (if applicable); Point of Contact (POC) name, phone number, and email address.
c. Confirmation of an 8(a) status

Evaluation: The FDA will evaluate to the extent that the Offeror provides the following information:

a. Reference to RFP #75F40126R00042
b. Company name; address; SAM UEI; Cage (if applicable); Point of Contact (POC) name, phone number, and email address.
c. Confirmation of an 8(a) status

VOLUME II: IDIQ TECHNICAL PROPOSAL INSTRUCTIONS & EVALUATION CRITERIA (50-page limit) (PHASE II)

The FDA's Advisory notification to offerors after evaluation of Phase I RFP submissions will include the due date for Phase II written submissions.

TAB A: FACTOR 2: IDIQ OVERALL UNDERSTANDING & APPROACH
Instructions: The Offeror shall provide a detailed narrative of it's understanding and approach to providing the requested IDIQ services. As a part of this narrative, include a "map" between the labor categories provided in the pricing spreadsheet (Attachment_A_Pricing Schedule and LCAT) and the labor categories. The map should demonstrate that labor categories proposal will encompass all of the technical expertise described in the FDA's suggest labor categories.

Evaluation: The FDA will evaluate the extent to which the Offeror's narrative demonstrates that it understands the requirement and has presented a logical, cohesive and technically sound approach to delivering the types of services required. FDA will evaluate whether the labor categories offered are appropriate to deliver the technical services described, and whether the resources proposed have the appropriate skills sets and certifications necessary to successfully perform.

TAB B: SUB FACTOR 1: APPROACH TO TASK ORDER #1 (Operations & Maintenance (O&M))
Instructions: The Offeror shall provide a detailed narrative of its understanding and approach to performing each of the tasks described in the Task Order 1 SOW with minimum interruption to business operations. The narrative should describe the Offeror's understanding of the project both from a technical and compliance standpoint.

TASK ORDER #1 TECHNICAL ASSUMPTIONS
Instructions: The Offeror shall identify any assumptions associated with the services to be performed for this Task Order.

TASK ORDER #1 DRAFT PROJECT MANAGEMENT PLAN AND WORK BREAKDOWN STRUCTURE
Instructions: The Offeror shall provide a draft project management plan for managing the activities under Task Order 1. The draft project management plan shall address the following areas: Requirements Management, Change Control, Risk Management, Schedule Management, Cost Management, Quality Management, Communications, and Project Organization. The Offeror shall also submit a Work Breakdown Structure (WBS) which identifies all the work requirements to perform the contract. Such a WBS shall be decomposed to a low enough level to permit evaluation of the Offeror's proposal. The Technical Proposal and the Task Order #1 Pricing shall be cross-referenced to the submitted WBS to facilitate evaluation.

TASK ORDER #1 STAFFING PLAN
Instructions: The Offeror shall complete the Task Order #1 Pricing (Attachment_A_Pricing Schedule and LCAT). The Task Order #1 Pricing shall identify the resources utilized, their qualifications and how they will be utilized across tasks. The instructions for completing the Task Order #1 Pricing are in the contained within the tab of the spreadsheet. The Offeror shall provide resumes that clearly identify education and experience of all personnel presented in the Task Order #1 Pricing. The resumes shall demonstrate the experience asserted in the Task Order #1 Pricing. Resumes are limited to (3) three pages for non-key personnel. If actual personnel have not yet been identified for non-key personnel, include representative resumes.

TASK ORDER #1 KEY PERSONNEL
Instructions: This section of the technical proposal shall identify key personnel and describe their specific roles in performing the activities in this Task Order.

In an appendix to the Staffing Approach marked Key Personnel, the Offeror shall submit resumes of key personnel. Resumes of staff and consultants shall reflect not only academic qualifications, but also length and variety of experience in similar tasks and clearly demonstrate relevant training and certifications. The Offeror shall clearly indicate whether the resumes submitted are those of current staff (subcontractor or prime) or are identified to be hired. If subcontractors are proposed, information shall be provided to support the qualifications of the subcontractors. The extent to which outside consultants or specialists will be used shall be documented and evidence of their availability shall be provided.

The Offeror shall provide resumes (limit 3 pages each) for individuals identified as key personnel. The Offeror shall provide letters of commitment for everyone identified as key personnel (limit 1 page each). Key Personnel must be available for assignment to this task order at task order award. The Offeror shall

also clearly indicate all proposed Key Personnel within its Staffing Plan. The Offeror shall indicate whether their project manager has been certified by the Project Management Institute or demonstrate clearly in narrative form that the candidate meets all the requirements of PMI certification.

TASK ORDER #1 OPERATIONS APPROACH
Instructions: The Offeror shall provide a detailed narrative describing its approach to:

- **24/7 system monitoring and incident response** for the mission-critical FARM system
- **Collaboration with Data Center Contractors and Cloud Environment providers** to identify and resolve system outages and performance issues
- **IT consolidation and modernization support**, including coordination with HALO, MARS, Elsa team, and Cloud environment teams
- **Security and compliance activities**, including Security Scans, COOP/ISCP exercises, and EDMSS compliance
- **Disaster recovery and business continuity** planning and execution
- **IT capacity planning and infrastructure management**, including monitoring data storage growth and infrastructure upgrades
- **Response time compliance** as outlined in the User Production Support Matrix

TASK ORDER #1 MAINTENANCE & DATABASE SUPPORT APPROACH
Instructions: The Offeror shall provide a detailed narrative describing its approach to:

- **Performance tuning and optimization** (biannual performance tuning to ensure optimal server capacity, speed, and network performance)
- **Workflow and application maintenance**, including maintenance and support of all FARM workflow applications and reports in the Cloud environment
- **Database administration and support**, including recommendations for database performance improvements, monitoring Oracle backups and recoveries, and maintaining user administration and role management
- **Submission processing and automation**, including recommendations for fully electronic submission processes
- **Support for agency-wide IT system consolidation efforts**

TASK ORDER #1 RELEASE MANAGEMENT & TESTING SUPPORT APPROACH
Instructions: The Offeror shall provide a detailed narrative describing its approach to:

- **Release development and management** for Initial, Major, Minor, and Emergency/Patch releases
- **Change Control Board (CCB) support**, including preparation of level of effort estimates, root cause analysis, and technical evaluation for defects and minor enhancements
- **User Acceptance Testing (UAT)** planning, support, and approval processes
- **Deployment coordination** with data center and Cloud environment contractors, including weekend and after-hours releases
- **Testing support**, including development of test plans, execution of functionality, regression, integration, performance, Section 508, and load tests
- **Defect tracking and resolution** using FDA tracking applications

TASK ORDER #1 USER PRODUCTION SUPPORT (HELPDESK) APPROACH
Instructions: The Offeror shall provide a detailed narrative describing its approach to:

- **Multi-tier user support** (Tier 1, 2, and 3) for the FARM platform

- **User account and access management**
- **Ticket management and resolution**, including achieving resolution rates consistent with historical performance
- **Communication and coordination** with Internal (FDA) users FDA help desk, other FDA personnel and external regulatory application submitters (industry COSM users),
- **Training and user guidance**, including one-on-one guidance and virtual training for external regulatory application submitters (COSM users)
- **Response time compliance** for different urgency levels as outlined in the User Production Support Matrix (Table 4)

TASK ORDER #1 SERVICE DELIVERY QUALITY ASSURANCE PLAN
Instructions: The Offeror shall provide a Service Delivery Quality Assurance Plan that clearly documents how the specific service levels in Table 4: User Production Support (FARM Helpdesk) Matrix within Attachment_2_TO1_SOW_OM will be assured.

TASK ORDER #1 RISK AND MITIGATION STRATEGIES
Instructions: The Offeror shall provide a narrative describing any risks it foresees carrying out its approach and mitigation strategies for those risks.

Evaluation: The FDA will evaluate the extent to which the Offeror's proposal demonstrates that it understands the requirement; has described tasks and procedures that are technically sound, logical, likely to be effective and will result in timely execution of the services; demonstrates a draft project management plan and WBS that is feasible and likely to result in the successful delivery of the services and deliverables on schedule and on budget; will provide the level of effort and labor mix of resources qualified, experienced, and capable of implementing the technical solution described; Quality Assurance Plan is technically sound, efficient, and likely to result in the successful measurement and attainment of quality services as identified in the User Support Matrix; and understands the risks associated with the services and has proposed strategies that will mitigate those risks.

TAB C: <u>TECHNICAL FACTOR 3:</u> MANAGEMENT APPROACH
Instructions: The Offeror shall provide a brief narrative describing how it intends to manage the IDIQ. This shall include a discussion of order management processes; staff availability; approach to client communication and collaboration, reporting, and the rationale for its approach.
The narrative shall identify personnel who will work on managing the IDIQ, their role in the project, and their qualifications. If the Offeror plans to form Contractor Teaming Arrangement(s) to provide an integrated solution to meet the Government's requirements, the Offeror shall submit copies of the Contractor Teaming Arrangement(s).

Evaluation: The FDA will evaluate the extent to which the Offeror's approach demonstrates that it can effectively manage a IDIQ of this magnitude. The FDA will evaluate each Offeror's management approach to ensure they have demonstrated the appropriate management infrastructure to manage multiple Task Orders, respond quickly and efficiently to new Task Order requests, and to attract and retain qualified personnel to staff the Task Orders.

<u>VOLUME III: TAB B: BUSINESS/PRICE PROPOSAL</u>

Instructions: The FDA will conduct price analysis on business proposals in accordance with actual prices and labor categories proposed for the services in the FDA Pricing Worksheet (Attachment_A_Pricing Schedule & LCAT).
Offeror's shall certify their proposal to be valid until **December 31, 2026**.
Offeror's shall submit pricing including unit pricing, for each item requested and total final price. Proposals shall clearly state the overall cost to the Government for all ordering periods.
Offeror's shall submit a proposal for all requirements listed in this RFP. Offerors are encouraged to submit their best pricing in their initial proposal. The Government intends to evaluate proposals based on the prices submitted and may make an award without discussions. Partial proposals will not be considered. Incomplete pricing or pricing with omissions may not be considered for award.
Rates shall remain the same for a 12-month Period of Performance (POP) and shall not change midstream of the Task Orde (TO) POP.
Offerors participating in teaming/partnering arrangements for this acquisition shall submit their teaming/partnering agreements with their proposal. The agreements shall be signed by the parties and shall demonstrate the relationship between firms and identify contractual relationships and authorities to bind the firm and the team/partnership. Offerors proposing major subcontracts (subcontracts exceeding 10% of the overall prime contract value) shall submit signed letters of commitment from the subcontractors which define the contractual relationship and identify contribution to the planned arrangement in terms of the type and proportion of work to be performed. Copies of agreements and letters of commitment shall be submitted with the proposal under this section and will not count towards the page limitation. Offerors shall include a cover page with their agreements to include a list of the teaming/partnering parties and the following information for each party: company name, SAM UEI, address, point of contact, email address, phone and fax numbers.

Evaluation: The Government will evaluate the Contractor's ability to deliver an efficient, low-risk proposal at a fair and reasonable price. As part of this evaluation, the Government will evaluate:

- Overall pricing for Task Order #1
- Pricing based on FDA provided labor categories and hours for all ordering periods. Please note that the Offeror will not be required to use these labor categories and annual hours for actual performance of each Task Order. Each Task Order will include labor categories and number of hours appropriate to the project. The hours listed are suggested figures for evaluation purposes only.

VOLUME III: TAB C: PROPOSAL ASSUMPTIONS, EXCEPTIONS, and DEPENDENCIES

Offeror's shall submit all assumptions in their proposal.
Offeror's must indicate, in this section only, if any pricing-related assumptions have been made, conditions have been stipulated or exceptions have been taken with this RFP or the Statement of Work as written. If assumptions are not noted in this Volume and this section of the proposal, it will be assumed that the firm's proposal reflects no assumptions for award and the firm agrees to comply with all of the terms and conditions set forth herein. It is not the responsibility of the Government to seek out and identify assumptions, conditions, or exceptions buried within the firm's proposal. Accordingly, any pricing related assumptions listed in any other volume or section shall be null and void. Any exceptions taken to the price-related terms and conditions of the RFP shall be stated in this Section. Any assumptions that are considered unacceptable by the Government and cannot be resolved may result in the firm being removed from consideration.

EVALUATION OF PROPOSAL:

The Government will assess its level of confidence that the Offeror will successfully perform the requirements of the contract in regard to the evaluation factors. The evaluation factors will measure the Government's confidence that the Offeror understands the requirements and will be successful in performing the contract. The evaluation will be done holistically with a rating scale of "high confidence," "moderate confidence," and "low confidence," representing the Government's confidence that the Offeror understands the requirement and will be successful in performing the work.

High Confidence	The Government has high confidence that the Offeror understands the requirement, has the ability to perform the scope based on the size, scope and complexity required by the Government, and will be successful in performing the contract with little or no Government intervention.
Moderate Confidence	The Government has some confidence that the Offeror understands the requirement, has the ability to perform the scope based on the size, scope and complexity required by the Government, and will be successful in performing the contract with some Government intervention.
Low Confidence	The Government has low confidence that the Offeror understands the requirement, has the ability to perform the scope based on the size, scope and complexity required by the Government, or will be successful in performing the contract even with Government intervention.

The non-price factors will be evaluated in descending order of importance as listed below.

- Factor 1: Relevant Experience Criteria (Phase I)
- Factor 2: IDIQ Overall Understanding & Approach (Phase II)
- Subfactor 1: Approach to Task Order (TO) #1 (Operations & Maintenance (O&M)) (Phase II)
- Factor 3: Management Approach (Phase II)

The non-price factors listed above will each be evaluated with a confidence rating of high, moderate or low. The non-price evaluation factor ratings will then receive an overall confidence rating of high, moderate or low.
The Government intends to award an IDIQ and one (1) task orders to the Offeror whose proposal conforms to the solicitation and represents the best value to the Government using tradeoffs, price and other factors considered. Evaluation Phase II and I are listed in descending order of importance and, when combined, are significantly more important than Volume III Cost. The evaluation will be based on the demonstrated capabilities of the Offeror in relation to the needs of the project as set forth in the RFP. The proposals will be evaluated carefully in accordance with the aforementioned confidence ratings to determine the best value to the Government. It is important the Offeror's proposal be submitted initially with the most favorable terms and include details to support the completed pricing in the Attachment_A_Pricing Schedule & LCAT because the Government intends to award without negotiation in accordance with FAR 52.215-1. However, the Government reserves the right to hold discussions, if the Government determines discussions are necessary.
This RFP does not commit the Government to pay any cost for the preparation and submission of a proposal. In addition, the Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds in connection with this proposed acquisition. The Government reserves the right to make administrative price/technical trade-offs that are in the best interest and to the advantage of the Government.

The Government will evaluate proposal for award purposes by adding the total price for all options (including the option to extend services) to the total price for the basic requirement. The Government may determine that a proposal is unacceptable if the option prices are significantly unbalanced. Evaluation of options shall not obligate the Government to exercise the option(s).

x. The clause at **52.212-4, Contract Terms and Conditions-Commercial Products and Commercial Services (APR 2026),** applies to this acquisition and with an addenda for invoicing procedures which can be found under *Attachment_1_IDIQ_SOW, section 4.6 Invoicing*.

xi. Additional Contract Requirements and Terms and Conditions

FAR CLAUSES

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 https://www.acquisition.gov/browse/index/far
(End of Clause)

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 *September 29, 2026,* through *September 28, 2031.*
(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.
(End of clause)

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 *$1,000*, 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*
(2) Any order for a combination of items in excess of *$25,000,000*; or
(3) A series of orders from the same ordering office within *14* 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 *three (3)* 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.

(End of clause)

52.216-22 Indefinite Quantity (NOV 2025)

(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 *five (5) years beyond the expiration of this IDIQ.*

(End of clause)

52.217-7 Option for Increased Quantity-Separately Priced Line Item (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor *any time before the contract expires*. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of clause)

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 6 months. The Contracting Officer may exercise the option by written notice to the Contractor *any time prior to the expiration date of the contract*.
(End of clause)

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 *any time prior to the expiration date of the* contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend *any time* before the contract expires. 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.
(End of clause)

52.219-17 Section 8(a) Award (OCT 2019)
(a) By execution of a contract, the Small Business Administration (SBA) agrees to the following:
(1) To furnish the supplies or services set forth in the contract according to the specifications and the terms and conditions by subcontracting with the Offeror who has been determined an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).
(2) Except for novation agreements, delegates to the [*Food and Drug Administration (FDA)]* the responsibility for administering the contract with complete authority to take any action on behalf of the Government under the terms and conditions of the contract; provided, however that the contracting agency shall give advance notice to the SBA before it issues a final notice terminating the right of the subcontractor to proceed with further performance, either in whole or in part, under the contract.
(3) That payments to be made under the contract will be made directly to the subcontractor by the contracting activity.
(4) To notify the *[Food and Drug Administration (FDA)]* Contracting Officer immediately upon notification by the subcontractor that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.
(5) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the cognizant Contracting Officer under the "Disputes" clause of the subcontract.
(b) The offeror/subcontractor agrees and acknowledges that it will, for and on behalf of the SBA, fulfill and perform all of the requirements of the contract.
(End of clause)

52.219-18 Notification of Competition Limited to Eligible 8(a) Participants (OCT 2022)
(a) Offers are solicited only from—
(1) Small business concerns expressly certified by the Small Business Administration (SBA) for participation in SBA's 8(a) program and which meet the following criteria at the time of submission of offer—
(i) The Offeror is in conformance with the 8(a) support limitation set forth in its approved

business plan; and
(ii) The Offeror is in conformance with the Business Activity Targets set forth in its approved business plan or any remedial action directed by SBA;
(2) A joint venture, in which at least one of the 8(a) program participants that is a party to the joint venture complies with the criteria set forth in paragraph (a)(1) of this clause, that complies with 13 CFR 124.513(c); or
(3) A joint venture—
(i) That is comprised of a mentor and an 8(a) protégé with an approved mentor-protégé agreement under the 8(a) program;
(ii) In which at least one of the 8(a) program participants that is a party to the joint venture complies with the criteria set forth in paragraph (a)(1) of this clause; and
(iii) That complies with 13 CFR 124.513(c).
(b) By submission of its offer, the Offeror represents that it meets the applicable criteria set forth in paragraph (a) of this clause.
(c) Any award resulting from this solicitation will be made to the Small Business Administration, which will subcontract performance to the successful 8(a) offeror selected through the evaluation criteria set forth in this solicitation. A contracting officer may consider a joint venture for contract award. SBA does not approve joint ventures for competitive awards, but see 13 CFR 124.501(g) for SBA's determination of participant eligibility.
(d) The _____ *[insert name of SBA's contractor]*shall notify the *[Food and Drug Administration (FDA)]* Contracting Officer in writing immediately upon entering an agreement (either oral or written) to transfer all or part of its stock.
(End of clause)

52.223-23 Sustainable Products (NOV 2025) (DEVIATION)
(a) *Definitions.* As used in this clause—
Sustainable product means—
(1) A product that contains recovered material designated by the EPA under the Comprehensive Procurement Guidelines (42 U.S.C. 6962) (40 CFR part 247)
(https://www.epa.gov/smm/comprehensive-procurement-guideline-cpg-program#products).
(2) An energy-efficient product or low standby power device (42 U.S.C. 8259b) (10 CFR part 436, subpart C) (https://www.energy.gov/eere/femp/search-energy-efficient-products, https://www.energystar.gov/products?s=mega,
and https://www.energy.gov/femp/low-standby-power-product-list).
(3) A biobased product that meets the content requirements of the USDA under the BioPreferred® program (7 U.S.C. 8102) (7 CFR Part 4270) (https://www.biopreferred.gov/).
(4) A substance identified in the EPA's Significant New Alternatives Policy (SNAP) program as a safe alternative to an ozone-depleting substance (42 U.S.C. 7671l) (40 CFR part 82, subpart G)
(https://www.epa.gov/snap/unacceptable-and-acceptable-substitutes-tables).

(b) *Requirements*. The Government has identified in the statement of work or elsewhere in the contract the sustainable products that are required during the performance of this contract. The Contractor shall ensure that it provides sustainable products as required by this contract, when the products are—
(1) Delivered to the Government;
(2) Furnished for use by the Government;
(3) Incorporated into the construction of a public building or public work; or

(c) Furnished for use in performing services under this contract, where the cost of the products is a direct cost to this contract.
(End of clause)

FAR Clause	Title	Date
52.202-1	Definitions	JUN 2020
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	JUN 2020
52.203-7	Anti-Kickback Procedures	JUN 2020
52.203-12	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
52.204-13	System for Award Management Maintenance	APR 2026
52.204-15	Service Contracting Reporting Requirements for Indefinite-Delivery Contracts	APR 2026
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	APR 2026
52.209-7	Information Regarding Responsibility Matters	APR 2026
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	APR 2026
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	APR 2026
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services	APR 2026
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services--Alternate I	APR 2026
52.219-6	Notice of Total Small Business Set-Aside	APR 2026
52.219-8	Utilization of Small Business Concerns	APR 2026
52.219-14	Limitations of Subcontracting	APR 2026
52.219-16	Liquidated Damages-Subcontracting Plan	APR 2026
52.219-28	Postaward Small Business Program Representations	APR 2026
52.222-3	Convict Labor	APR 2026
52.222-19	Child Labor-Cooperation with Authorities and Remedies	APR 2026
52.222-35	Equal Opportunity for Veterans	APR 2026
52.222-36	Equal Opportunity for Workers with Disabilities	APR 2026
52.222-37	Employment Reports on Veterans	APR 2026
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	APR 2026
52.222-41	Service Contract Labor Standards	APR 2026
52.222-50	Combating Trafficking in Persons	APR 2026
52.222-54	Employment Eligibility Verification	APR 2026
52.222-55	Minimum Wages for Contractor Workers Under Executive Order 14026	APR 2026

52.222-62	Paid Sick Leave Under Executive Order 13706	APR 2026
52.222-90	Addressing DEI Discrimination by Federal Contractors	APR 2026
52.224-3	Privacy Training	JAN 2017
52.226-8	Encouraging Contractor Policies to Ban Text Messaging While Driving	MAY 2024
52.227-1	Authorization and Consent	JUN 2020
52.232-23	Assignment of Claims	MAY 2014
52.232-29	Terms for Financing of Purchases of Commercial Products and Commercial Services	NOV 2021
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
52.233-3	Protest After Award	APR 2026
52.233-4	Applicable Law for Breach of Contract Claim	APR 2026
52.240-92	Security Requirements	APR 2026
52.240-93	Basic Safeguarding of Covered Contractor Information Systems	APR 2026
52.242-5	Payments to Small Business Subcontractors	JAN 2017
52.242-15	Stop – Work Order	AUG 1989
52.245-1	Government Property	SEP 2021
52.245-1	Government Property--Alternate I	APR 2012
52.245-9	Use and Charges	APR 2012

52.252-6 Authorized Deviations in Clauses (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any *Health and Human Services Acquisition Regulation* (48 CFR *Chapter 3*) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

HHSAR CLAUSES

The full text of a Health and Human Services Acquisition Regulation (HHSAR) clause may be accessed electronically at this/these address(es):
https://www.hhs.gov/grants/contracts/contract-policies- regulations/hhsar/part-352-solicitation-provisions-contract-clauses/index.html.

352.203-70 Anti-Lobbying (JUN 2026) (DEVIATION)

Pursuant to the HHS annual appropriations acts, except for normal and recognized executive-legislative relationships, the Contractor shall 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 subsections (a), (b), and (c) above shall 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)

352.204-71 Information and Information Systems Security (FEB 2024) (DEVIATION)

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

Breach means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where—

(1) A person other than an authorized user accesses or potentially accesses personally identifiable information, or

(2) An authorized user accesses personally identifiable information for an other than authorized purpose.

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

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

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

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

(4) *Business associate* includes the following:

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

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

(iii) A subcontractor that creates, receives, maintains, or transmits protected

health information on behalf of the business associate.
(5) *Business associate* does not include:
(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.
(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) apply and are met.
(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.
(iv) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement by virtue of such activities or services.
Business associate agreement means the agreement, or other arrangement, as dictated by the HIPAA Privacy Rule (45 CFR 160), between an HHS covered entity and a business associate, which must be entered into in addition to the underlying contract for services and before any disclosure (see 45 CFR 160.103) of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of an HHS entity.
Controlled unclassified information (CUI) means information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information.
Healthcare component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with 45 CFR 164.105(a)(2)(iii)(D) (see 45 CFR 164.103). The Secretary of HHS has designated HHS as a covered entity (further designated as a "hybrid entity"), and has also designated four HHS divisions as healthcare components under HIPAA, including —
(1) The Centers for Medicare and Medicaid Services (CMS), insofar as it operates the fee-for-service Medicare program;
(2) The Program Support Center (PSC), Division of Commissioned Personnel, insofar as it operates a health plan for Commissioned Corps officers;
(3) The World Trade Center (WTC) Health Program; and,
(4) The Indian Health Service (IHS), insofar as it operates a health plan and a program providing healthcare that uses electronic transactions.
HHS Information Technology General Rules of Behavior means a set of HHS rules that describes the responsibilities and expected behavior of users of HHS information or information systems.
HHS sensitive information means all HHS data, on any storage media or in any form or format, which requires confidentiality, integrity, and availability protection due to the risk of harm that could result to interests of HHS, other agencies or entities, or individuals from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes—
(1) Information where the improper use or disclosure could adversely affect the ability of HHS to accomplish its mission, *i.e.*, HHS proprietary information;
(2) Records about individuals requiring protection under laws and regulations such as the E-Government Act, Privacy Act and the HIPAA Privacy Rule, or based on a data use agreement or a promise or assurance of confidentiality; and

(3) Information that would be exempt from disclosure if requested under the Freedom of Information Act. Examples of HHS sensitive information include—
(i) Individually-identifiable medical, benefits, and personnel information;
(ii) Financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, security-sensitive, procurement-sensitive, investigatory, and law enforcement information;
(iii) Controlled unclassified information;
(iv) Information that would be confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and
(v) Other information which, if released, could result in a violation of law or agreement, could cause harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.
HIPAA Rules means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and part 164.
Incident means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies.
Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.
Information technology (see FAR 2.101) also means Information and Communication Technology (ICT).
Information technology-related contracts means those contracts that include services (including support services), and related resources for information technology.
Organized health care arrangement (see 45 CFR 160.103) means:
(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement;
and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

(3) A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
(4) A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
(5) The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.
Privacy officer means the HHS official(s) with responsibility for implementing and oversight of privacy related policies and practices that impact a given HHS acquisition.
(b) *General*. Contractors, subcontractors, their employees, third-parties, and business associates with access to HHS information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to the HHS Cybersecurity Program and the directives and handbooks, complete HHS security training prior to accessing HHS information (including HHS sensitive information and information systems security and privacy) and on an annual basis thereafter, as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, HHS *Personnel Security and Suitability Program*, which establishes HHS procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards, and guidance for protecting HHS information, information systems (see 302.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing HHS information or information systems.
(c) *Access to HHS information and HHS information systems*.
(1) Contractors are limited in their request for logical or physical access to HHS information or HHS information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery, or purchase orders.
(2) All Contractors, subcontractors, third parties, and business associates working with HHS information are subject to the same investigative requirements as those of HHS appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors to access HHS information and HHS information systems shall be in accordance with HHS *Personnel Security and Suitability Program*.
(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.
(4) The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling*" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be –
(i) Marked appropriately;
(ii) Disclosed to authorized personnel on a need-to-know basis;
(iii) Protected in accordance with NIST SP 800-53, *Security and Privacy*

Controls for Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* if handled by internal Contractor system; and

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

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

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

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

the covered entity and the prime contractor.

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

(e) *Roster of employees.* Contractors and subcontractors shall provide a roster containing the name, position, e-mail address, phone number, and responsibilities of each employee, including subcontractors, performing work under the contract to develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to Contracting Officer within [*30*] days stated number of days from the effective date of the contract. Revisions to the roster as a result of staffing changes must be submitted within the number of days of the change provided by the Contracting Officer. The Contracting Officer, or the Contracting Officer's Representative (COR), will notify the Contractor of the appropriate level of investigation required for each staff member based on the information provided on the roster. If an employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level.

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

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

(h) *HHS information custodial requirements*.

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

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

requirements. The Contractor and subcontractor will provide all necessary access and support to HHS and/or GAO staff during periodic control assessments or audits.

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

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

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

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

(7) *Violation of information custodial requirements*. If HHS determines that the Contractor has violated any of HHS information confidentiality, privacy, or security provisions, it shall be sufficient grounds for HHS to withhold payment to the Contractor or third-party or

terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

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

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

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

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

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

(j) *Report of known or suspected incident or breach*. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify HHS immediately via the

Contracting Officer and the COR or within one (1) hour of a known or suspected incident or breach. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. Report all actual or suspected incident and breach information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than an agreed upon days which will be set at the time the known or suspected incident or breach is discovered. 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 *FDA patch management policy timeframes.*

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

(k) *Incident and breach investigation*.

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

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

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

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

(l) *Incident and breach notification requirements*.

(1) The Contractor/subcontractor shall provide notice to HHS of an incident as set forth in the incident and breach investigation section of this clause. The Contractor shall fully cooperate with HHS or third- party entity performing an independent risk analysis on behalf of HHS. Failure to cooperate may be deemed a material incident or breach and grounds for contract termination.
(2) The Contractor/subcontractor shall fully cooperate with the HHS Computer Security Incident Response Center (CSIRC), HHS Breach Response Team, Operating Divisions (OPDIVs), Staff Divisions (STAFFDIVs), other stakeholders or any Government agency conducting an analysis regarding any notice of an incident or breach, potential incident or breach, or incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for HHS, and shall address all relevant information concerning the incident or breach, including the following:
(i) Nature of the event (loss, theft, unauthorized access).
(ii) Description of the event, including:
(A) Date of occurrence.
(B) Date of incident or breach detection.
(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.
(D) Number of individuals affected or potentially affected.
(E) Names of individuals or groups affected or potentially affected.
(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.
(G) Amount of time the data has been out of HHS control.
(H) The likelihood that the sensitive information will or has been compromised (made accessible to and usable by unauthorized persons).
(I) Known misuses of data containing sensitive information, if any.
(J) Assessment of the potential harm to the affected individuals.
(K) Incident or breach analysis as outlined in the HHS Breach Response Policy and Plan, as appropriate.
(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive information that may have been compromised.
(M) Steps taken in response to mitigate or prevent a repetition of the incident.
(m) *Training*.
(1) All Contractor employees and subcontractor employees requiring access to HHS information or HHS information systems shall complete the following before being granted access to HHS information and its systems:
(i) On an annual basis, successfully complete the HHS Privacy and Information Security Awareness and HHS Information Security Rules of Behavior training.
(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the HHS Information Security Rules of Behavior, relating to access to HHS information and information systems.
(iii) Successfully complete any additional cyber security or privacy training, as required for HHS personnel with equivalent information system access.
(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that HHS Information Security Rules of Behavior signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

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

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

(End of clause)

352.204-72 Records Management (FEB 2024) (DEVIATION)

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

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

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

(1) The term Federal record—

(i) Includes HHS records;

(ii) Does not include personal materials;

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

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

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

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

(c) *Requirements.*

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

(2) In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5

U.S.C. 552), and the Privacy Act of 1974 (5 U.S.C. 552a), and must be managed and scheduled for disposition only as permitted by statute or regulation.

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

(4) The Contractor is responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation. Federal records may not be removed from the legal custody of HHS or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Contracting Officer. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. The Contractor shall report to the Contracting Officer any unlawful or accidental removal, defacing, alteration, or destruction of Federal records.

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

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

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

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

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

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

(End of Clause)

352.204-73 Contractor Personnel Security and Agency Access (FEB 2024) (DEVIATION)

(a) Definitions. As used in this clause—

Agency access means access to HHS facilities, sensitive information, information systems or other HHS resources.
Applicant means a contractor employee for whom the Contractor applies for an HHS identification card.
Contractor employee means a prime contractor and subcontractor employee who requires agency access to perform work under an HHS contract.
Identification card (or "ID card") means a government issued or accepted identification card such as a Personal Identity Verification (PIV) card, a PIV-Interoperable (PIV-I) card from an authorized PIV-1 issuer, or a non-PIV card issued by HHS, or a non-PIV card issued by another Federal agency and approved by HHS. PIV and PIV-1 cards have physical and electronic attributes that other (non-PIV) ID cards do not have.
Issuing office means the HHS entity that issues identification cards to contractor employees.
Local security servicing organization means the HHS entity that provides security services to the HHS organization sponsoring the contract.
(b) Risk and sensitivity level designations. For contracts requiring access to HHS facilities, sensitive information, information systems or other HHS resources, contractor employees will be required to complete background investigations, identity proofing, and government identification card application procedures to determine suitability for access. HHS will assign a risk and sensitivity level designation to the overall contract and/or to contractor employee positions by category, group or individual. The risk and sensitivity level designations will be the basis for determining the level of personnel security processing required for contractor employees. The position sensitivity designation levels that apply will be identified in the contract. The following risk and sensitivity level designations and associated level of processing are required, and each level includes the prior levels—

(1) Low risk level: National Agency Check with Written Inquiries (NACI);
(2) Moderate risk level: Minimum Background Investigation (MBI); and
(3) High risk level: Background Investigation.

(c) Security clearances. Contractor employees may also be required to obtain security clearances (i.e., Confidential, Secret, or Top Secret). National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive," will determine the level of clearance required for contractor employees. Personnel security clearances for national security contracts in HHS will be processed according to the HHS Personnel Security and Suitability Program, HHS Instruction 731-1, and the Department of Defense National Industrial Security Program Operating Manual (NISPOM).
(d) Pre-screening of contractor employees. The Contractor must pre-screen individuals designated for employment under any HHS contract by verifying minimal suitability requirements to ensure that only candidates that appear to meet such requirements are considered for contract employment, and to mitigate the burden on the Government of conducting background investigations on objectionable applicants. The Contractor must exercise due diligence in pre-screening all employees prior to submission to HHS for agency access. HHS may decline to grant agency access to a contractor employee for reasons including, but not limited to—

(1) Conviction of a felony, a crime of violence, or a misdemeanor involving moral turpitude;
(2) Falsification of information entered on forms or of other documents submitted;
(3) Improper conduct including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct adverse to the Government regardless of whether the conduct is directly related to the contract; and
(4) Any behavior judged to pose a potential threat to HHS facilities, sensitive information, information systems or other resources.

(e) Citizenship status. The Contractor must monitor a non-citizen’s continued authorization for employment in the United States. The Contractor must provide documentation to the Contracting

Officer or the Contracting Officer's Representative (COR) during the background investigation process that validates that the E-Verify requirement has been met for each contractor employee.

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

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

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

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

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

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

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

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

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

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

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

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

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

(ii) Failure to comply with the requirements for custody and control of HHS ID cards may result in withholding final payment or contract termination based on the potential for serious harm caused by inappropriate access to HHS facilities, sensitive information, information systems or other HHS resources.

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

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

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

(C) Replacement. An ID card will be replaced if it is damaged, contains incorrect data, or is lost or stolen for more than 3 days, provided there is a

continuing need for agency access to perform work under the contract.

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

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

352.208-70 Printing and Duplication (FEB 2026) (DEVIATION)

(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 shall[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)

352.224-71 Confidential Information (FEB 2024) (DEVIATION)

(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 advance 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: *Any confidential data other than that of the Contractor*.

(2) The reason(s) for restricting the types of information identified in subparagraph (d)(1) is/are: *any basis valid under the Freedom of Information Act, including, but not limited to: Information related solely to the internal personnel rules and practices of an agency; Information that is prohibited from disclosure by another federal law; Trade secrets or commercial or financial information that is confidential or privileged; Privileged communications within or between agencies; and Information that, if disclosed, would invade another individual's personal privacy*.

(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)

352.231-70 Salary Rate Limitation (FEB 2026) (DEVIATION)

(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 website 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)

352.232-71 Electronic Submission of Payment Requests (APR 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)

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 individuals are considered to be essential to the work being performed and are designated as key personnel:

Name	**Title**
To be determined at task order level	*To be determined at task order level*

(End of clause)

352.239-71 Security Requirements for Information Technology Resources (FEB 2024) (DEVIATION)
(a) *Definitions*. As used in this clause—
Information technology has the same meaning in FAR 2.101.
Information and communication technology (ICT) also means information technology (see FAR 2.101 for definitions).
Information system security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.
(b) *Responsibilities*. The Contractor shall be responsible for information technology security for all systems connected to a Department of Health and Human Services (HHS) network or operated by the Contractor for HHS, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or other system access to HHS information that directly supports the mission of HHS. Examples of tasks that require security provisions include—
(1) Hosting of HHS e-Government sites or other information technology operations;
(2) Acquisition, transmission, or analysis of data owned by HHS with significant replacement cost should the contractor's copy be corrupted; and
(3) Access to HHS general support systems/major applications at a level beyond that granted the general public, e.g., bypassing a firewall.
(c) *Information system security plan*. The Contractor shall develop, provide, implement, and maintain an Information System Security Plan. HHS information system and platform information technology systems must have a security plan that provides an overview of the security requirements for the system and describes the security controls in place or the plan for meeting

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

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

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

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

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

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

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

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

(g) *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).

(h) *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.

(i) *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.

(j) *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.

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

(End of clause)

352.239-73 Information System Design and Development (FEB 2024) (DEVIATION)

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

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

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

fixes shall not negatively impact the Systems.

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

(End of clause)

352.239-74 Information System Hosting, Operation, Maintenance, or Use (FEB 2024) (DEVIATION)

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

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

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

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

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

must be submitted and approved prior to the collection of PII.

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

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

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

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

(1) Completion or termination of the contract; or

(2) Disposal or return of the IT equipment by the Contractor/subcontractor or any person acting on behalf of the Contractor/subcontractor, whichever is earlier.

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

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

(1) The Contractor must accept the system without the drive;
(2) A spare drive must be installed in place of the original drive at time of turn- in if HHS initial medical device purchase included a spare drive; or
(3) The Contractor may request reimbursement for the drive at a reasonable open market replacement cost to be separately negotiated by the Contracting Officer and the Contractor at time of contract closeout.

(End of clause)

352.239-75 Security Controls Compliance Testing (FEB 2024) (DEVIATION)

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

(End of clause)

352.239-76 Security Requirements for Government-Owned Contractor- Operated and Contractor-Owned Contractor-Operated Resources (FEB 2024) (DEVIATION)

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

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

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

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

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

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

(b) *Assessment and Authorization (A&A).* A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) of *30 business days.* The Contractor must conduct the A&A requirements in accordance with *HHS*

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 within *30 business days* 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 *30 business days After Receipt of Order.* 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 10 business days after award The security assessment must be conducted by *the Contracting Officers Representative (COR)* assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with the COR shall conduct, or as directed, in the assessment of the security controls 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 prior to the application going live. 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 within 15 business days 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) High -15, Moderate -30, Low -60 business days from the date the weaknesses are formally identified and documented;

(B)

Critical-risk weaknesses must be mitigated within 15 business days from the date the weaknesses are formally identified and documented;

(C) High-risk weaknesses must be mitigated 15 business days from the date the weaknesses are formally identified and documented;

(D)

Medium weaknesses must be mitigated within 30 business days from the date the weaknesses are formally identified and documented; and

(E)

Low weaknesses must be mitigated within 60 business 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 monthly.

(3)

A Contingency Plan and Contingency Plan Test are due annually. 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 as needed. 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 as needed on an ongoing basis.

(10) *Patching and vulnerability remediation*. The Contractor shall install vendor- released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

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

(12) *Boundary protection.* The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection.

(13) *Government access for security assessment*.

(i) In addition to the Inspection Clause in the contract, the Contractor shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of

federal data or to the protection of information systems operated on behalf of HHS. This access includes, but is not limited to—

(1) At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, access to Contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. For the purposes of this paragraph only, *Government* includes, but is not limited to, Contracting Officer, COR, the U.S. Department of Justice, U.S. Government Accountability Office, and the HHS Office of the Inspector General (OIG). The purpose of access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include, but not be limited to, such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, Structured Query Language injection vulnerabilities, and any other known vulnerabilities.

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

(ii) The Contractor shall segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Government inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

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

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

(d) *Desktops, laptops, and other computing devices required for use by the Contractor.* The Contractor shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of HHS are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

(1) Encrypt equipment and sensitive information stored and/or processed by such equipment

in accordance with HHS encryption standard and current FIPS 140 validation certificate from the NIST Cryptographic Module Validation Program.
(2)
Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline, *30 business days* and HHS Minimum Security Configuration Standards;
(3) Maintain the latest operating system patch release and anti-virus software definitions at least for the life of the contract;
(4) Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
(5) Automate configuration settings and configuration management in accordance with HHS security policies, including but not limited to:
(i) Configuring its systems to allow for periodic HHS vulnerability and security configuration assessment scanning; and
(ii) Using SCAP-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the Contracting Officer and/or COR, Project Officer, and any other point of contract designated by the Contracting Officer or COR.
(e) *Rights to data.* Contractors shall specify any data rights asserted and mark such deliverables accordingly in accordance with applicable data rights clauses set forth in the contract.
(f) *Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements*. The Contractor shall secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232, section 889. At a minimum, the Contractor shall—
(1) Develop rules for suppliers' development methods, techniques, or practices;
(2) Use secondary market components;
(3) Prohibit counterfeit products;
(4) Dispose and/or retain elements such as components, data, or intellectual property securely;
(5) Ensure adequate supply of components;
(6) Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
(7) Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
(8) Establish Service Level Agreements (SLAs), patching vehicles, and disclosure requirements in the case of an incident or new vulnerability being discovered; and
(9) Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
(10) Prohibit the use of covered telecommunications and video surveillance equipment or services.
(g) *Subcontract flow down*. The Contractor shall include the substance of this clause, including this paragraph (g), in subcontracts and third-party agreements, at any tier, of any amount and in which subcontractor employees and third-party servicers/employees, will perform functions or provide products under the scope of this contract, and have access to HHS information (including HHS sensitive information, *i.e.*, protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see HHSAR 302.101, Definitions).

(End of clause)

352.239-77 CLOUD COMPUTING SERVICES (FEB 2024) (DEVIATION)

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

(1) *Federal Risk and Authorization Management Program (FedRAMP) compliant authorization to operate.* Compliance with FedRAMP Assessment and Authorization (A&A) requirements and ensure the information system/service (see HHSAR 302.101, Definitions) under this contract has an approved FedRAMP compliant authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO prior to use at FDA. An FDA ATO shall be conducted prior to app being available for FDA to use.

(i) Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline available at fedramp.gov). The *HHS Policy for Information Security and Privacy Protection (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall implement additional controls identified by the agency in this contract.

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

(2) *Data jurisdiction.* The Contractor shall store all information within the security authorization boundary, data at rest, or data backup, within the Continental United States, when applicable.

(3) *Service Level Agreements (SLAs)*. When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and the cloud service provider and work with the Contracting Officer's Representative (COR) to develop and maintain an SLA, as provided in the contract.

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

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

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

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

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

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

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

(ii) Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

(5) The disposition of all HHS data shall be at the written direction of the COR. This may include documents returned to HHS control, destroyed, or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(i) If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements contained within FAR 52.224.

(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: FedRamp package must be available

(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.

(5) Revocation of a cloud service. HHS has the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information (see HHSAR 302.101, Definitions), HHS may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the internet, other networks, or applying additional security controls.

(d) *Reporting and continuous monitoring.*

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

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

(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 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 one (1) hour. 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 based on the criticality of the vulnerability.

(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) (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)

352.239-79 Information and Communication Technology Accessibility (FEB 2024) (DEVIATION)
(a) Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998, all information and communication technology (ICT) supplies, products, platforms, information, documentation, and services support developed, acquired, maintained or delivered under this contract or order must comply with the Revised 508 Standards, which are located at 36 C.F.R. 1194.1 and Appendices A, B, and C, and are available at https://www.access-board.gov/ict/. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html.
(b) Additional Section 508 accessibility standards applicable to this contract or order may be identified in the specification, statement of work, or performance work statement. If it is determined by the Government that ICT supplies, products, platforms, information, documentation, and services support provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies, products, platforms, information, documentation, or services support to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(c) In the event of a modification(s) to this contract or order, which adds new ICT supplies or services or revises the type of, or specifications for, supplies, products, platforms, information, documentation, or services support, the Contracting Officer shall require that the Contractor submit a completed HHS Section 508 Accessibility Conformance Checklist (see https://www.hhs.gov/web/section-508/accessibility-checklists/index.html) or an Accessibility Conformance Report (ACR) (based on the Voluntary Product Accessibility Template (VPAT) see https://www.

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

FAR/HHSAR PROVISIONS

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 this/these address(es):
https://acquisition.gov/far/
(End of provision)

FAR Provision	Title	Date
52.204-7	System for Award Management	NOV 2025
52.209-7	Information Regarding Responsibility Matters	NOV 2025
52.212-1	Instructions to Offerors—Commercial Products and Commercial Services	NOV 2025
52.215-1	Instructions to Offerors-Competitive Acquisition	NOV 2025
52.216-27	Single or Multiple Awards	OCT 1995

52.216-31	T&M/LH Proposal Requirements—Commercial Acquisition	NOV 2021
52.217-5	Evaluation of Options	NOV 2025
52.219-31	Notice of Small Business Reserve	MAR 2020
52.229-11	Tax on Certain Foreign Procurements—Notice and Representation	APR 2026

52.252-5 Authorized Deviations in Provisions (NOV 2020)
(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.
(b) The use in this solicitation of any *Health and Human Services Acquisition Regulation* (48 CFR *Chapter 3*) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.
(End of provision)

HHSAR

The full text of a Health and Human Services Acquisition Regulation (HHSAR) provision may be accessed electronically at this/these address(es):
https://www.hhs.gov/grants/contracts/contract- policies-regulations/hhsar/part-352-solicitation-provisions-contract-clauses/index.html.

352.239-72 Information System Security Plan and Accreditation (FEB 2024) (DEVIATION)
All offers submitted in response to this solicitation or request for quotation shall address the approach for completing the security plan and accreditation requirements in clause 352.239-71, Security Requirements for Information Technology Resources.
(End of provision)

352.239-78 INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE (FEB 2024)(DEVIATION)
(a) Any offeror responding to this solicitation must comply with established HHS Information and Communication Technology (ICT) accessibility standards. Information about Section 508 is available at https://www.hhs.gov/web/section-508/index.html. 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)

xii. The Defense Priorities and Allocations System (DPAS) and assigned rating is **NOT** applicable.

xiii. Phase I & Phase II Proposal Due Dates & Times:

Phase I: Volume I: Relevant Experience Submission Due Date
Offeror's shall submit a written response electronically in PDF format via email to address the Phase I items that is no greater than six (6) pages excluding the cover page to the Contract Specialist, Brian Wodzisz at Brian.Wodzisz@fda.hhs.gov, and the Contracting Officer, Peter Lee at Peter.Lee@fda.hhs.gov, **by 3:00pm (Eastern) on August 14th, 2026.** The subject line shall read: "75F40126R00042– Food Applications Regulatory Management (FARM) IDIQ." Late submissions may not be evaluated. Fax submissions are not authorized. Each Offeror will receive an Advisory Notification.

Phase II: Volume II Proposal Submission Due Date
The Phase II submission due date and time will be provided in the Advisory Notification letter. Offeror's shall submit a written response electronically in PDF format via email to the Contract Specialist, Brian Wodzisz at Brian.Wodzisz@fda.hhs.gov and the Contracting Officer, Peter Lee at Peter.Lee@fda.hhs.gov. The subject line shall read: "75F40126R00042– Food Applications Regulatory Management (FARM)

IDIQ." Late submissions may not be evaluated. Fax submissions are not authorized.

It is the Offeror's responsibility to monitor SAM.Gov for the release of an amendment to the combined synopsis/solicitation (if any).

Offeror's that fail to complete the required representations and certifications, or reject the terms and conditions of the solicitation, may be excluded from consideration. It is the responsibility of the Offeror to ensure that submissions are received by the FDA by the due dates and times indicated.

xiv. Points of Contact:

Contract Specialist (CS): Brian Wodzisz – Brian.Wodzisz@fda.hhs.gov
Contracting Officer (CO): Peter Lee – Peter.Lee@fda.hhs.gov