Date: May 18, 2022

From: Janae Hughes, Contract Specialist, Facilities Support Branch, OAGS

Subject: Request for Quote

Identification Number: **75F40122Q00040**

NAICS Code: 334516

SMALL BUSINESS SET-ASIDE

A. BACKGROUND AND OBJECTIVE

The Food and Drug Administration (FDA) is responsible for ensuring that all personnel who may encounter radiological sources or material are properly protected. Currently, the FDA has a need for the use of an onsite X-Ray machine on our Muirkirk Road Campus (MRC) for diagnostic testing of potential musculoskeletal injuries to our animals while they are onsite. During operations of the X-Ray machine FDA Center for Veterinary Medicine Office of Research (CVM OR) personnel may be exposed to low levels of X-Ray radiation and it is necessary to capture exposure levels during these operations through the use of personnel dosimetry badges.

B. STATEMENT OF WORK (SOW) -- SCOPE OF WORK

The U.S. Food and Drug Administration (FDA) seeks to acquire **Whole Body and Finger Ring Dosimetry Badge Services** for a base year and four (1) year options. The Government intends to award a Firm Fixed-Price Purchase Order for the requirements described in line items number (LIN) 1-5. The Vendor shall indicate if the minimum salient characteristics have been met to be considered responsive for this requirement.

Minimum Required Salient Characteristics

The services shall include the following:

1) The Contractor shall provide the shipment of five (5) whole body and ring dosimetry badges directly to the MRC.
2) The Contractor shall provide CVM and/or technical point of contact (TPOC) the ability of tracking dosimetry badges and reports to ensure that badges correspond to the assigned individuals over the course of the monitoring period. After returning badges back to Contractor, reports detailing potential exposure levels must be available within ten business days.
    a. Reports at the minimum shall provide radiation exposure for the quarter per badge by each employee.

b. Reports shall also detail radiation exposure trending over the course of the contract to allow for the CVM Safety Team to determine if any radiation dosage changes require procedure modifications.

3) The Contractor shall supply each individual badge labeled with unique identifiable labels. to ensure proper tracking.
4) The means to return each badge back to the Contractor shall supply the postage mail delivery within five business days on a quarterly basis for dose reporting.
5) The means to access quarterly radiation dose reports electronically and confidentially through a secured website.
6) The Contractor shall provide replacement of any badge that may be physically damaged during the quarterly testing period within two business days.
7) The Contractor shall provide CVM with one body and one ring dosimetry for 5 employees (CVM/OR Safety Coordinator, two Attending Veterinarians, and two sets as spares).

Other Requirements

1) If any of the Contractor's personnel must come onsite to the MRC, they will be treated as a visitor and must be escorted by an FDA employee while onsite.
2) Contractor's coming onsite to FDA buildings will need to either check the community levels on their own or reach out to the Occupational Safety and Health Officer prior to coming onsite for up-to-date masking guidance. COVID community transmission levels can be accessed HERE (www.cdc.gov).
3) If the Contractor visits any rooms or buildings on the CVM OR campus, the contractor must agree to be escorted at all times and abide by all national consensus standards for safety and security including National Institutes of Health, Occupational Safety and Health Administration and the Nuclear Regulatory Commission in addition to any CVM specific safety and security policies and procedures.
4) Instructions to offerors:
    a. Quotes shall include costs for replacements in the event badges are lost by FDA or damaged if replacement is not included at no additional cost. Replacements may be paid for via PCard transaction.
    b. Quotes shall include any costs for replacement badges and specific labels as necessary for spares in the event of FDA employee turnover.
    c. Quotes shall include whether any Personally Identifiable Information (PII) is required from the FDA for performance of this contract. It is anticipated that CVM will be able to provide the contractor with unique identifiers for the badges in lieu of sharing of PII information (i.e. Individual A, Individual B, etc.). In addition, quotes need to include details on how FDA information will be retrieved

and stored. This information is needed so FDA can access if the Privacy Act applies to this contract. If it is found to apply, additional requirements related to the Privacy Act will be included on this contract.

Deliverables

During the duration of the contract, the Contractor shall accomplish the following:

1) Supply reports of radiation exposure within ten business days of the end of each quarterly reporting period via electronic and through a secured website.
2) Badges for each subsequent quarterly reporting period are delivered to the OR location prior to the start period for the corresponding reporting period.
3) Provide resources for mail delivery return of dosimetry badges within five business days of CVM OR shipping the assigned badges back to the Contractor at the end of each quarterly reporting period.
4) Provide replacement badges for any physically damaged badges within two business days of request
5) The means to access quarterly radiation dose reports electronically and through a secured website.
6) Technical support for any questions related to the dosimetry program as needed during standard business hours via phone and/or email (9:00AM-5:00PM, M-F). It is expected that if the phone or email contact does not have the requisite expertise to answer inquiries, they have the ability to contact an individual with the necessary expertise by the end of the next business day.

C. PERIOD OF PERFORMANCE

Base Year: 6/6/2022-6/5/2023
Option Year 1: 6/6/2023-6/5/2024
Option Year 2: 6/6/2024-6/5/2025
Option Year 3: 6/6/2025-6/5/2026
Option Year 4: 6/6/2026-6/5/2027

D. PLACE OF PERFORMANCE

8401 Muirkirk Rd
Building MOD2
Laurel, MD 20708

E. LINE ITEM AND PRICES

All charges must be included in the quote. Any charges presented after contract award shall be unacceptable.

LIN	DESCRIPTION	QTY	PRICE
1	Whole Body and Ring Dosimetry Services Period of Performance: 6/6/2022-6/5/2023	5 EA	$
2	Option Year 1: Whole Body and Ring Dosimetry Services Period of Performance: 6/6/2023-6/5/2024	1 YR	$
3	Option Year 2: Whole Body and Ring Dosimetry Services Period of Performance: 6/6/2024-6/5/2025	1 YR	$
4	Option Year 3: Whole Body and Ring Dosimetry Services Period of Performance: 6/6/2025-6/5/2026	1 YR	$
5	Option Year 4: Whole Body and Ring Dosimetry Services Period of Performance: 6/6/2026-6/5/2027	1 YR	$
Grand Total = *Firm-Fixed Price*			$

F. IT SECURITY/PRIVACY REQUIREMENTS

NOTE to Contractor: Before the purchase order is awarded, FDA is required to get pre-approval of all the IT hardware and/or software-firmware-freeware from the FDA Chief Information
Officer (CIO). For IT hardware, this includes any device that processes or stores data, or is controlled by data (computers/data switches, etc.), but does not include passive hardware (rack, network cables, power supplies/cords, etc.). This will require the applicable Vendor to **provide a complete list of hardware and/or software-firmware-freeware that the Vendor will use in fulfilling this purchase order.**

This list will need to include:

1. IT hardware: manufacture, nomenclature and model number
2. Software (all types): manufacture, nomenclature and version number

Item(s) rejected by the CIO will need to be changed and the replacement item(s) would need to go through the same approval process.

A. Baseline Security Requirements

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

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

   b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the HHS mission. In addition to the Federal Acquisition Regulation

(FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

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

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

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

b. Provide security for any Contractor systems, and information contained therein, connected to an FDA network or operated by the Contractor on behalf of FDA regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, within one (1) hour or less, bring the situation to the attention of the other party. This includes notifying the FDA Systems Management Center (SMC) within one (1) hour of discovery/detection in the event of an information security incident.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS/FDA Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the FDA Information Security Program security requirements, outlined in the FDA Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing your ISSO.

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

3) Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, Appendix C, and based on information provided by the ISSO or other security

representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality: [ ] Low [X] Moderate [ ] High
Integrity: [ ] Low [X] Moderate [ ] High
Availability: [ ] Low [X] Moderate [ ] High
Overall Risk Level: [ ] Low [X] Moderate [ ] High
Based on information provided by the Privacy Office, system/data owner, or other privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [X] Yes PII

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

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

4) Controlled Unclassified Information (CUI). CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa). As implemented the term "*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. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

a. marked appropriately;

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

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

d. returned to FDA control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, *Guidelines for Media Sanitization* and the FDA IS2P Appendix T: *Sanitization of Computer-Related Storage Media*.

5) Protection of Sensitive Information. For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution.

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

The confidentiality, integrity, and availability of such information shall be protected in accordance with //HHS and *FDA* policies. Unauthorized disclosure of information will be subject to the HHS/*FDA* sanction policies and/or governed by the following laws and regulations:

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

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

7) Government Websites. All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade

connections to plain HTTP. For internal-facing websites, the HTTPS is not required, but it is highly recommended.

8) Contract Documentation. The Contractor shall use FDA-provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

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

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

b. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.

c. All devices (i.e.: desktops, laptops, mobile devices, etc.) that store, transmit, or process non-public FDA information should utilize FDA-provided or FDA information security authorized devices that meet HHS and FDA-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

d. Verify that the encryption solutions in use are compliant with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR.

e. Use the Key Management system on the HHS Personal Identification Verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys (PIV card) shall be provided to the COR upon request and at the conclusion of the contract. Upon completion of contract, contractor ensures that COR is able to access and read any encrypted data.

10) Contractor Non-Disclosure Agreement (NDA). Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the FDA non-disclosure agreement (3398 Form), as applicable. A copy of each signed and witnessed NDA shall be submitted to the CO and/or COR prior to performing any work under this acquisition.

11) Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) – The Contractor shall assist the procuring activity representative, program office and the FDA SOP or designee

with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

a. If the results of the PTA show that a full PIA is needed, the Contractor shall assist procuring activity representative, program office and the FDA SOP or designee with completing a PIA for the system or information after completion of the PTA and in accordance with HHS and FDA policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. The PTA/PIA must be completed and approved prior to active use and/or collection or processing of PII and is a prerequisite to agency issuance of an authorization to operate (ATO).

b. The Contractor shall assist the procuring activity representative, program office and the FDA SOP or designee in reviewing and updating the PIA at least every *three years* throughout the Enterprise Performance Life Cycle (EPLC) /information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

B. Training

1) Mandatory Training for All Contractor Staff. All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable FDA Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete FDA Information Security Awareness, Privacy, and Records Management training at least *annually*, during the life of this contract. All provided training shall be compliant with HHS and FDA training policies.

2) Role-based Training. All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the program manager) must complete role-based training *annually* commensurate with their role and responsibilities in accordance with HHS and FDA policy and *FDA Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Standard Operating Procedures (SOP).*

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

C. Rules of Behavior

1) The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior*.

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

D. Incident Response

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

FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines incidents as events involving cybersecurity and privacy threats, such as viruses, malicious user activity, loss of, unauthorized disclosure or destruction of data, and so on.

A privacy breach is a type of incident and is defined by FISMA as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS *Policy for IT Security and Privacy Incident Reporting and Response* further defines a breach as "a suspected or confirmed incident involving PII."

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

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

2) NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the

Contractor shall send FDA approved notifications to affected individuals as directed by FDA's SOP.

3) Report all suspected and confirmed information security and privacy incidents and breaches to the FDA Systems Management Center, COR, CO, and other stakeholders, (Recommend adding the FDA Senior Official for Privacy with contact information and either defining or deleting "other stakeholders.") including incidents involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than one (1) hour of discovery/detection, and consistent with the applicable FDA and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contract information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor shall:

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

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

c. encrypt sensitive information in attachments to email, media, etc.

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

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

E. Position Sensitivity Designations

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

N/A for this contract.

F. Homeland Security Presidential Directive (HSPD)-12

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

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

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

G. Contract Initiation and Expiration

1) General Security Requirements. The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the FDA EPLC framework and methodology in accordance with the FDA EPLC Project documentation, located here:
http://sharepoint.fda.gov/orgs/DelMgmtSupport/IntakeProc/EPLCv2/SitePages/v2/EPLCHome.aspx
HHS EA requirements may be located here:
https://www.hhs.gov/about/agencies/asa/ocio/index.html

2) System Documentation. Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

3) Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all

required documentation in accordance with FDA OAGS SMGs to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization and FDA IS2P Appendix T: *Sanitization of Computer-Related Storage Media*

4) Notification. The Contractor (and/or any subcontractor) shall notify the CO and/or COR as soon as it is known that an employee will stop working under this contract.
5) Contractor Responsibilities Upon Physical Completion of the Contract. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or FDA policies.

6) The Contractor (and/or any subcontractor) shall coordinate with the COR via email, copying the Contract Specialist, to ensure that the appropriate person performs and documents the actions identified in the FDA eDepart system http://inside.fda.gov:9003/EmployeeResources/NewEmployee/eDepartDepartureSystem/default.htm as soon as it is known that an employee will terminate work under this contract within days of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

H. Records Management and Retention

The Contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and HHS/FDA policies and shall not dispose of any records unless authorized by HHS/*FDA*.

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

A. Security Requirements for GOCO and COCO Resources

1) Federal Policies The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *FDA Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and*

Organizations; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

2) Security Assessment and Authorization (SA&A). A valid authorization to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s). The Contractor shall conduct the SA&A requirements in accordance with *FDA IS2P*, NIST SP 800- 37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (latest revision).

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

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

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

i. System Security Plan (SSP) – due a week prior to the start of the annual security assessment. The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and FDA policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system, as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least *annually* thereafter.

ii. Security Assessment Plan/Report (SAP/SAR) – due before the system is made available to standard users. The security assessment shall be conducted by FDA's team of security assessors, unless otherwise noted and be consistent with NIST SP 800-53A, NIST SP 800-

30, and HHS and FDA policies. The assessor will document the assessment results in the SAR.

iii. Independent Assessment – This shall be coordinated through the FDA Information Security program.

iv. POA&M – due as part of the SAR. The POA&Ms shall be documented consistent with the HHS and FDA Standard for Plan of Action and Milestones and FDA policies. All high-risk weaknesses must be mitigated within *30 calendar days* and all medium weaknesses must be mitigated within *60 calendar days* from the date the weaknesses are formally identified and documented. FDA's assessors will determine the risk rating of vulnerabilities.

Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as noted in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, FDA may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least *quarterly.*

v. Contingency Plan and Contingency Plan Test – due before the start of the annual security assessment. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,* and be consistent with HHS and FDA policies. Upon acceptance by the System Owner, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned and any action items that need to be addressed. Thereafter, the Contractor shall update and test the Contingency Plan at least annually.

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

Based on the level of assurance determined by the E-Auth, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the E- Auth (when required) in accordance with HHS and FDA policies.

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems

that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and FDA IS2P. The following are the minimum requirements for ISCM:

i. Annual Assessment/Pen Test - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or an FDA-authorized independent third-party for all high impact systems. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date in the deliverable table.

ii. Asset Management - Using an FDA-approved Security Content Automation Protocol (SCAP)-compliant automated tool for active/passive scans, provide an inventory of all information technology (IT) assets for hardware and software, (computers, servers, routers, databases, operating systems, etc.) that are processing FDA-owned information/data. It is anticipated that this inventory information will be required to be produced at least annually to facilitate management/oversight efforts). IT asset inventory information shall include IP address, machine name, operating system level, security patch level, and SCAP- compliant format information. The contractor shall maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.

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

iv. Vulnerability Management - Use FDA-approved SCAP-compliant automated tools for authenticated
scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS and FDA policy. Automated tools shall be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor shall maintain a capability to provide security vulnerability scanning information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least monthly.

v. Patching and Vulnerability Remediation - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and FDA specified timeframes (follow the FDA patch management policy).

vi. Secure Coding - Follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), that will limit system software vulnerability exploits.

vii. Boundary Protection - The contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities is routed through a Trusted Internet Connection (TIC).

3) Government Access for Security Assessment. In addition to the Inspection Clause in the contract, the Contractor (and/or any subcontractor) shall afford the Government access to the Contractor's facilities, installations, operations, documentation, information systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of HHS, including but are not limited to:

a. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract.

The Government includes, but is not limited to, the U.S. Department of Justice, U.S. Government Accountability Office, the HHS Office of the Inspector General (OIG), and FDA Information Security. The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include, but not be limited to, such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, SQL injection vulnerabilities, and any other known vulnerabilities.

b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full

cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

c. Segregate Government protected information and metadata on the handling of Government protected information from other information. Commingling of information is prohibited. Inspectors, auditors, and investigators will not be precluded from having access to the sought information if sought information is commingled with other information.

d. Cooperate with inspections, audits, investigations, and reviews.

4) End of Life Compliance. The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version. The contractor shall retire and/or upgrade all software/systems that have reached end-of- life in accordance with FDA *End-of-Life Operating Systems, Software, and Applications Policy*.

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

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

b. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), FDA Configuration Baselines, and FDA Minimum Security Configuration Standards;

c. Maintain the latest operating system patch release and anti-virus software definitions, per FDA patch management policy;

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

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

i. Configuring its systems to allow for periodic Federal vulnerability and security configuration assessment scanning; and
ii. Using FDA-approved Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capabilities to scan its systems at least on a *monthly* basis and report the results of these scans to the CO and/or COR, and any other applicable designated POC.

G. GOVERNMENT HOLIDAYS

a. The Government hereby provides notification that Government personnel observe the listed days as holidays:

A. New Year's Day
B. Martin Luther King's Birthday
C. President's Day
D. Memorial Day
E. Juneteenth National Independence Day Observance
F. Independence Day
G. Labor Day
H. Columbus Day
I. Veterans' Day
J. Thanksgiving Day
J. Christmas Day

b. In addition to the days designated as holidays, the Government observes the following days:

(1) Any other day designated by Federal Statute
(2) Any other day designated by Executive Order
(3) Any other day designated by the President's Proclamation

c. When any such day falls on a Saturday, the following Monday is observed. Except for designated around-the-clock or emergency operations, Contractor personnel will not be able to perform on-site under this contract with FDA on holidays set forth above. The Contractor will not charge any holiday as direct charge to the award.

d. It is understood and agreed between the Government and the Contractor that observance of such days by Government personnel shall not otherwise be a reason for an additional period of performance, or entitlement of compensation except as set forth within the award.

e. Nothing in this clause abrogates the rights and responsibilities of the parties relating to stop work provisions as cited in other sections of this contract.

H. EVALUATION AND AWARD

The Government shall award this contract to the Lowest Priced, Technically Acceptable (LPTA). The Government reserves the right to award an order without discussions if the Contracting Officer determines that the initial offer is providing the Best Value and discussions are not necessary.

I. INSTRUCTIONS TO OFFEROR FOR PROPOSAL SUBMISSION

FAR 52.212-1 Instructions to Offerors—Commercial Items (NOV 2021)

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.

PROPOSAL SUBMISSION FORMAT

*****Proposal shall be in 2 volumes: 1 Technical and 2 Price. The volumes shall be separate and complete. The volumes shall be separate and complete, so that evaluation of one may be accomplished independently of, and concurrently with, the evaluation of the other. No pricing information shall be provided in volume 1.*****

The total number of pages for the technical quote shall not exceed fifteen (15) pages, using 1" margins, single spaced, font type Time New Roman, and a font size of 12.

*******The solicitation does not commit the Government to pay any cost for the preparation and submission of a quote or proposal. It is also advised that the Contracting Officer (CO) is the only individual who can legally commit and obligate the Government to the expenditure of public funds in connection with the proposed acquisition.***

Offeror agrees to hold the prices in its offer firm through September 30, 2022.

QUESTIONS DEADLINE: Interested offerors shall submit questions electronically to janae.hughes@fda.hhs.gov no later than May 31, 2022, 12:00 PM Eastern Time. Please include the company name, FDA solicitation number, and "Question(s)" in the subject line.

No Phone Calls Please.

PROPOSAL DUE: All proposals are due, electronically to contract specialist email: Janae.hughes@fda.hhs.gov for the RFQ no later than June 3, 2022, 12:00 PM Eastern Time.

J. PROVISIONS AND CLAUSES

52.212-4 -- Contract Terms and Conditions -- Commercial Items. Contract Terms and Conditions -- Commercial Items (Nov 2021).

FAR 52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services (May 2022)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with *Alternate I* (Nov 2021) (41 U.S.C. 4704 and 10 U.S.C. 2402).

__ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509)).

__ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

__ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

__ (5) [Reserved].

__ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

__ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

__ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Nov 2021) (31 U.S.C. 6101 note).

__ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

__ (10) [Reserved].

__ (11) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Sep 2021) (15 U.S.C. 657a).

__ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Sep 2021) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

__ (13) [Reserved]

_x_ (14) (i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-6.

__ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

__ (ii) Alternate I (Mar 2020) of 52.219-7.

__ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

__ (17) (i) 52.219-9, Small Business Subcontracting Plan (Nov 2021) (15 U.S.C. 637(d)(4)).

__ (ii) Alternate I (Nov 2016) of 52.219-9.

__ (iii) Alternate II (Nov 2016) of 52.219-9.

__ (iv) Alternate III (Jun 2020) of 52.219-9.

__ (v) Alternate IV (Sep 2021) of 52.219-9.

__ (18) (i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

__ (ii) Alternate I (Mar 2020) of 52.219-13.

__ (19) 52.219-14, Limitations on Subcontracting (Sep 2021) (15 U.S.C. 637s).

__ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Sep 2021) (15 U.S.C. 637(d)(4)(F)(i)).

__ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Sep 2021) (15 U.S.C. 657f).

__ (22) (i) 52.219-28, Post Award Small Business Program Rerepresentation (Sep 2021) (15 U.S.C. 632(a)(2)).

__ (ii) Alternate I (Mar 2020) of 52.219-28.

__ (23) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Sep 2021) (15 U.S.C. 637(m)).

__ (24) 52.219-30, Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Sep 2021) (15 U.S.C. 637(m)).

__ (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

__ (26) 52.219-33, Nonmanufacturer Rule (Sep 2021) (15U.S.C. 637(a)(17)).

__ (27) 52.222-3, Convict Labor (Jun 2003) (E.O.11755).

__ (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Jan 2022) (E.O.13126).

__ (29) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

__ (30) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O.11246).

__ (ii) Alternate I (Feb 1999) of 52.222-26.

__ (31) (i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

__ (ii) Alternate I (Jul 2014) of 52.222-35.

__ (32) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

__ (ii) Alternate I (Jul 2014) of 52.222-36.

__ (33) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

__ (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

_X_ (35) (i) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).

__ (ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

__ (36) 52.222-54, Employment Eligibility Verification (May 2022) (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR 22.1803.)

__ (37) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

__ (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).

__ (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

__ (40) (i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

__ (ii) Alternate I (Oct 2015) of 52.223-13.

__ (41) (i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (Jun 2014) (E.O.s 13423 and 13514).

__ (ii) Alternate I (Jun2014) of 52.223-14.

__ (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (May 2020) (42 U.S.C. 8259b).

__ (43) (i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

__ (ii) Alternate I (Jun 2014) of 52.223-16.

__ (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020) (E.O. 13513).

__ (45) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).

__ (46) 52.223-21, Foams (Jun2016) (E.O. 13693).

__ (47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).

__ (ii) Alternate I (Jan 2017) of 52.224-3.

__ (48) 52.225-1, Buy American-Supplies (Nov 2021) (41 U.S.C. chapter 83).

__ (49) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (Nov 2021) (41 U.S.C.chapter83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43.

__ (ii) Alternate I (Jan 2021) of 52.225-3.

__ (iii) Alternate II (Jan 2021) of 52.225-3.

__ (iv) Alternate III (Jan 2021) of 52.225-3.

__ (50) 52.225-5, Trade Agreements (Oct 2019) (19 U.S.C. 2501, *et seq*., 19 U.S.C. 3301 note).

_x_ (51) 52.225-13, Restrictions on Certain Foreign Purchases (Feb 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

__ (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302Note).

__ (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

__ (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov2007) (42 U.S.C. 5150).

__ (55) 52.229-12, Tax on Certain Foreign Procurements (Feb 2021).

__ (56) 52.232-29, Terms for Financing of Purchases of Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

__ (57) 52.232-30, Installment Payments for Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

_X_ (58) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct2018) (31 U.S.C. 3332).

__ (59) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

__ (60) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

__ (61) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

_X_ (62) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).

__ (63) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631).

__ (ii) Alternate I (Apr 2003) of 52.247-64.

__ (iii) Alternate II (Nov 2021) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

__ (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter67).

__ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

__ (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (May 2014) (29U.S.C.206 and 41 U.S.C. chapter 67).

_X_ (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

__ (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

__ (7) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).

__ (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).

__ (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR 2.101, on the date of award of this contract, and does not contain the clause at 52.215-2, Audit and Records-Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the

Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial products or commercial services. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Nov 2021) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2015) (E.O.11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May2014) (41 U.S.C. chapter 67).

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xvi) 52.222-54, Employment Eligibility Verification (May 2022) (E.O. 12989).

(xvii) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).

(xviii) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).

(xix)

(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

52.217-5 Evaluation of Options (Jul 1990)

Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. Evaluation of options will not obligate the Government to exercise the option(s).

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 before the contract expires.

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 before the contract expires*;* provided that the Government gives the Contractor a preliminary written notice of its intent to extend 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 5 years.

HHSAR CLAUSES

HHSAR Clauses Incorporated by Reference

302.101	Definitions (Dec 2015)
352.211-3	Paperwork Reduction Act (Dec 2015)
352.222-70	Contractor Cooperation in Equal Employment Opportunity Investigations (Dec 2015)
352.239-74	Electronic Information and Technology Accessibility (Dec 2015)

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

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

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

c.

1. The Agency will enroll the Contractors new to IPP. The Contractor must follow the IPP registration email instructions for enrollment to register the Collector Account for submitting invoice requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive Registration email from the Federal Reserve Bank of St. Louis (FRBSTL) within 3 - 5 business days of the contract award for new contracts or date of modification for existing contracts.
2. Registration emails are sent via email from ipp.noreply@mail.eroc.twai.gov. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email to IPPCustomerSupport@fiscal.treasury.gov or phone (866) 973-3131.
3. The Contractor POC will receive two emails from **IPP Customer Support**, the first email contains the initial administrative IPP User ID. The second email, sent within 24 hours of receipt of the first email, contains a temporary password. You must log in with the temporary password within 30 days.
4. If your company is already registered to use IPP, you will not be required to re-register.
5. If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment as authorized by HHSAR 332.7002, a written request must be submitted to the Contracting Officer to explain the circumstances that require the authorization of alternate payment procedures.

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

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

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

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

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

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

(b) total amount of all payments received to date under the subject contract or order
(c) and, for definitized contracts or orders only, total estimated amounts yet to be invoiced for the current, active period of performance.

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

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

i. Payment to the Contractor will not be made for temporary work stoppage due to circumstances beyond the control of U.S. Food and Drug Administration such as acts of

God, inclement weather, power outages, and results thereof, or temporary closings of facilities at which Contractor personnel are performing. This may, however, be justification for excusable delays.

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

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

GENERAL INFORMATION

CONTRACTING POINT OF CONTACT:
Janae Hughes
Contract Specialist
Email: janae.hughes@fda.hhs.gov