REQUEST FOR QUOTATION

(THIS IS NOT AN ORDER)

THIS RFQ [X] IS [ ] IS NOT A SMALL BUSINESS SET ASIDE

PAGE 1 OF PAGES 43

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG.1	RATING
75F40124Q00463	08/05/2024			

5a. ISSUED BY
DHHS/FDA/OAGS/DAO
ATTN: Ian Weiss
10903 New Hampshire Ave.
WO2/3rd Floor
Silver Spring MD 20903

6. DELIVERY BY (*Date*)
Multiple

7. DELIVERY
[X] FOB DESTINATION [ ] OTHER (*See Schedule*)

9. DESTINATION
a. NAME OF CONSIGNEE

b. STREET ADDRESS

c. CITY

d. STATE e. ZIP CODE

5b. FOR INFORMATION CALL: (*No collect calls*)

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
IAN WEISS		

8. TO:

a. NAME b. COMPANY

c. STREET ADDRESS

d. CITY e. STATE f. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS (*Date*)
08/16/2024 1530 ET

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.

11. SCHEDULE (*Include applicable Federal, State and local taxes*)

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	This is a Request for Quotation (RFQ) is for Whole Genome Sequencing for FDA/CVM in support of a study. See attached RFQ. Period of Performance: 09/09/2024 to 09/08/2025				

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations [ ] are [ ] are not attached

13. NAME AND ADDRESS OF QUOTER
a. NAME OF QUOTER

b. STREET ADDRESS

c. COUNTY

d. CITY e. STATE f. ZIP CODE

14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION

15. DATE OF QUOTATION

16. SIGNER
a. NAME (*Type or print*)

b. TELEPHONE AREA CODE NUMBER

c. TITLE (*Type or print*)

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

Title: Whole Genome Sequencing for FDA/CVM in support of a study

The U.S. Food & Drug Administration (FDA), Center for Veterinary Medicine/Office of Applied Science/Division of Applied Veterinary (CVM/OAS/DAVR) has a requirement to provide **Whole Genome Sequencing**

PRICING SCHEDULE

CLIN	Description	Quantity	Cost Each	Total Cost
0001	gDNA extraction	**34**	**$**	**$**
0002	library prep and sequencing	**34**	**$**	**$**
0003	Shipping/Freight (wgs)	**4**	**$**	**$**
TOTAL COST				**$**

1. **Background**
   Upon completion of targeted gene editing, FDA/CVM/OAS/DAVR requires whole genome sequencing of our samples in order to perform analyses to determine the unintended alterations that occurred, both at the intended target site and elsewhere in the animal genome. This acquisition is for whole genome sequencing services; FDA/CVM does not have the equipment to perform this work in-house in a timely and cost-effective manner.

2. **Objectives**
   The objective of this acquisition is for a contractor to perform whole genome sequencing for FDA/CVM/OAS/DAVR in support of a study. The whole genome sequencing is to provide accurate sequencing of edited and control pig genomes, which are approximately 2.7 Gb long. This will allow us to determine the changes to the genome that resulted from the CRISPR/Cas9 mediated editing events.

3. **Scope**
   As a result of this contract, CVM/OAS/DAVR expects to receive 30x whole genome sequence of submitted pig cell samples.

4. **Requirements**
   The requirement of this contract is to perform whole genome sequencing.

4.1 For whole Genome sequencing, the contractor shall meet the following requirements at

a minimum:

- CVM/OAS will provide all cell and tissue samples and the contractor shall supply all reagents necessary for all steps taking place at the contractor's facility.
- Library prep kit shall be able to use as little as 100ng of DNA input.
- Facility shall state status of CLIA and CAP accreditations.
- For successful completion of this work, the following tasks are anticipated. The minimum requirements for each task are outlined below. The contractor shall elaborate on their technical approach to these tasks as part of the proposal.
- **4.1.1 Provide Shipping Costs and Materials:**
    - If the contractor's sequencing facility is not within 30 miles of FDA/CVM's Laurel, MD campus, the whole genome sequencing samples shall be shipped with an easily trackable, overnight carrier on dry ice. These samples will be shipped such that they will arrive Tuesday, Wednesday, or Thursday, unless the sequencing facility is open on Saturdays, in which case, samples will be shipped to arrive Tuesday, Wednesday, Thursday, or Friday.
    - Shall supply the costs and any specialized materials to ship the samples from 8401 Muirkirk Rd, Laurel, MD 20708 to the contracted sequencing facility.
    - Shall receive the samples in a maximum of four shipments, with the shipment sizes being either 20 samples at once or 10 samples, 5 samples, and then the last 5 samples.
    - Shall send shipment information within 3 business days of notification that samples are ready to ship.
- **4.1.2 Isolate gDNA from Mammalian Cell Sample:**
    - Shall extract DNA from 34 pig cell line and tissue samples.
    - DNA shall be double stranded and non-degraded with a DNA integrity number, as measured by an Agilent Bioanalyzer or equivalent, of >7.0 and a A260/280 >/= 1.7.
- **4.1.3 Prepare Sequencing Libraries of Samples for Whole Genome Sequencing:**
    - Shall generate 34 sequencing libraries using the extracted gDNA and the Illumina Truseq DNA nano (550) kit. If needed, an alternate Illumina kit can be suggested for review by the TPOC.
- **4.1.4 Run Quality Control on Sample Libraries:**
    - Sequencing libraries will pass nucleic acid quantity, quality, and integrity control checks
- **4.1.5 Sequence Sample Libraries:**
    - Shall sequence the 34 generated libraries on an Illumina NovaSeq platform using 150 bp paired end reads to a depth sequencing coverage of at least 30X, with each sample yielding approximately 85 Gb raw throughput.
    - All reads must be generated from the same sequencing platform.
    - All reads for a given sample must be generated on the same instrument.
- **4.1.6 Determine Sequence Quality:**
    - Upon sequencing libraries passing quality control, 80% of the reads shall have a Q score above 30. If not, contractor shall assume costs to repeat any sequencing runs.
    - At minimum, an aggregate of 85Gb (30x) of sequencing data per sample must pass FastQC quality metrics for per base sequence quality, per tile sequence

quality, per sequence quality scores, per base sequence content, per base N content, per base N content, sequence length distribution, sequence duplication levels, overrepresented sequences, and adapter content.
    - If 85Gb of data do not pass, sequencing shall be repeated, on the same instrument, until the 85Gb threshold is reached.
- **4.1.7 Deliver Raw Sequencing Reads (fastq files):**
    - Shall transfer all raw sequencing data to CVM via precisionFDA (https://precision.fda.gov/) to a folder that will be communicated after the contract is awarded
      OR
    - Shall make samples available for sFTP transfer to the FDA/CVM

Task Number	Work Milestones	Turnaround Time
4.1.1	Provide shipping costs and materials	3 business days from request
4.1.2	Isolate gDNA from mammalian cell sample	1 week
4.1.3	Prepare sequencing libraries of samples for whole genome sequencing	1 week
4.1.4	Run quality control on sample libraries	1 week
4.1.5	Sequence sample libraries	8 weeks
4.1.6	Determine sequence quality	1 week
4.1.7	Deliver raw sequencing reads (fastq files)	1 week

For Task 4.1.2 of the above table, the turnaround time begins upon sample receipt. For tasks 4.1.3 to 4.1.7 of the above table, the task turnaround time begins upon completion of the prior task. For example, if task 4.1.2 is completed in 3 days (Day 3), task 4.1.3 should be completed in a week starting from Day 4.

5. Deliverables

The contractor shall provide the following:
1) shall upload, or make available for sFTP transfer, the full untrimmed raw read files in the format of fastq for the 34samples to the FDA hosted high performance computing platform - precisionFDA (https://precision.fda.gov/).
2) shall provide information about how the data was generated (DNA extraction method, library preparation method, sequencing method, quality control method, instrument run parameters, base calling).
3) shall deliver the raw reads within 13 weeks of sample receipt, unless the original samples do not pass quality control. In order to pass the quality control, all sections of 4.1.6 Determine Sequence Quality must be met.

6. Place of Performance

The contract will be performed at the Contractor's facility.

7. Place of Performance

The period of performance: 9/9/2024 - 9/8/2025

8. Inspection and Acceptance

All items specified in this Requirements Statement to be delivered under this order are subject to final inspection and acceptance by an authorized representative for the Government. The authorized representative of the Government is the Government's COR, who is responsible for inspection and acceptance of all services, materials, or supplies to be provided by the Contractor.

The COR will coordinate with FDA's bioinformatician, who runs the raw data through an analysis pipeline and verifies the sample quality. The COR will provide written notification of acceptance or rejection within 10 days of receipt. The Contractor shall correct any deficiencies within thirty (30) days of when the Government issues the rejection notice. If the Contractor cannot correct the deficiencies within this time frame, the Contractor shall immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) business days.

9. Contract Type

Firm-Fixed price (FFP).

10. Security Requirement

1. Baseline Security Requirements

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

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

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

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

i. Protect the:

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

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

- **Confidentiality:** [X] Low [ ] Moderate [ ] High
- **Integrity:** [ ] Low [X] Moderate [ ] High
- **Availability:** [X] Low [ ] Moderate [ ] High
- **Overall Impact Level:** [ ] Low [X] Moderate [ ] High

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

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

v. Adopt and implement all applicable policies, procedures, controls, and standards required by the FDA Information Security Program to ensure the confidentiality,

integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the FDA Information Security Program security requirements, outlined in the FDA Information Security and Privacy Protection (IS2P) policy, by contacting the CO/COR or emailing your ISSO.

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

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

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

ii. Based on information provided by the ISSO, System/Data Owner, or other security or privacy representative, it has been determined that this solicitation/contract involves: [X] No PII [ ] PII

iii. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed. If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information after completion of the PTA and in accordance with HHS and FDA policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. The PTA/PIA must be completed and approved prior to active use and/or collection or processing of PII and is a prerequisite to agency issuance of an authorization to operate (ATO).

- The Contractor must support the agency in reviewing the PIA at least every ***three years*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

e. **Controlled Unclassified Information (CUI). Executive Order 13556 defines** CUI as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The Contractor (and/or any subcontractor) must comply with *Executive Order 13556, Controlled Unclassified Information, (implemented at 3 CFR,* part 2002*)* when handling CUI. 32 C.F.R. 2002.4(aa) As implemented the term "*handling"* refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of

the information." 81 Fed. Reg. 63323. The requirements below apply only to nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. All sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, must be:

i. Marked appropriately;

ii. Disclosed to authorized personnel on a Need-To-Know basis;

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

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

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

g. Government Furnished Equipment (GFE) for Foreign Travel. FDA personnel are prohibited from taking GFE when participating in personal, unofficial travel to foreign countries. FDA personnel are strictly prohibited from teleworking using GFE in foreign countries. FDA personnel must also request loaner GFE from the FDA Foreign Travel program for official travel to any foreign country. Please see the FDA IS2P, *Appendix T Government Furnished Equipment for Foreign Travel*.

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

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

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

iii. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

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

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

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

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

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

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

ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with an encryption solution that is validated with current FIPS 140 validation certificates from the NIST CMVP.

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

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

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

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

2. Training Requirements

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

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

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

3. Rules of Behavior

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

b. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Agency data or other information, systems, and/or networks that

store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter, which may be done as part of annual FDA Information Security Awareness Training. If the training is provided by the contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

4. Incident Response

a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/FDA CIOCC /Incident Response Team teams **within 24 hours,** whether the response is positive or negative. FISMA defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*, an incident is "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the FDA IS2P Appendix F: Incident Response and the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."

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

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

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

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

point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:

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

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

- Encrypt sensitive information in attachments to email, media, etc.

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

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

5. Position Sensitivity Designations All Contractor (and/or any subcontractor) employees must obtain a background investigation commensurate with their position sensitivity designation that complies with Parts 1400 and 731 of Title 5, Code of Federal Regulations (CFR). The following position sensitivity designation levels apply to this solicitation/contract (e.g. tier 1, 2, or 4): **Not Applicable for this acquisition.**

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

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

8. Contract Initiation and Expiration

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

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

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

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

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

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

FDA Information Technology Procurements - Security and Privacy Language 33
performs and documents the actions identified in the FDA eDepart system.

9. Records Management and Retention

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

b. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS and FDA policies.

10. High Value Asset (HVA) If a system is identified as HVA,24 the contractor must comply with the FDA IS2P Appendix AB: High Value Asset (HVA) Program, the HHS Policy for the High Value Asset (HVA) Program, and the DHS HVA Control Overlay25 in addition to the above requirements.

All documentation must be available to the CO and/or COR upon request.

1. Security Requirements for GOCO and COCO Resources

a. **Federal Policies.** The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS and FDA policies that include, but are not limited to, the *HHS Information Security and Privacy Protection (IS2P)* policy; *FDA Information Security and Privacy Protection (IS2P) policy*; *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, Departmental, and Agency policies.
b. **Assessment and Authorization (A&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s): *[Within 30 days].* The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ FDA IS2P* NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision). FDA acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

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

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

- **Security Assessment Plan/Report (SAP/SAR)** - due before the system is made available to standard users. The security assessment must be conducted by FDA's team of security assessors, unless otherwise noted and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and FDA policies. The assessor will document the assessment results in the SAR. Thereafter, the Contractor, in coordination with FDA, must assist in the assessment of the security controls and update the SAR at least ***annually***. A copy of the updated SAR should be provided if requested.

- **Independent Assessment** - The Contractor (and/or subcontractor) must have an independent third party validate the security and privacy controls in place for the system(s) commensurate with the risk levels per NIST SP 800-53B. The independent third party must review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor must address all "high" deficiencies *and* enter all other deficiencies that require mitigation by Contractor before submitting the package to the Government for acceptance and document all remaining deficiencies in a system Plan of Action and Milestones (POA&M).

- **POA&M** - as part of the SAR All high-risk weaknesses must be mitigated within 30 calendar days moderate weaknesses must be mitigated within 60 calendar days and low weaknesses must be mitigated within 180 calendar days from the date the weaknesses are formally identified and documented. Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, flaws and security defects in a system (that require to create a patch for remediation), and other security reviews and sources, as documented in the SAR, must be documented and tracked by the Contractor for mitigation in the POA&M document consistent with the HHS Standard for Plan of Action and Milestones, FDA POA&M Management Guide, and FDA IS2P policies. Depending on the severity of the risks, FDA may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, continue to remediate weaknesses throughout the contract. The POA&M document must be updated at least **quarterly**

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

- **E-Authentication Questionnaire** - The contractor (and/or any subcontractor) must collaborate with government personnel to ensure that the E-Authentication requirements are implemented in accordance with OMB 04-04 and NIST SP 800-63 B. Based on the level of assurance determined by the E-Auth, the Contractor (and/or

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

ii. **Information Security Continuous Monitoring.** Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, must meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137*, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, HHS ISCM Strategy, and HHS and FDA IS2Ps.

iii. **Annual Assessment/Penetration (Pen) Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this involves penetration testing conducted by the FDA. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date in the deliverable table.

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

v. **Configuration Management** - Use FDA-approved SCAP-compliant automated tools as per NIST IR 7511 and *HHS Minimum Security Configurations Standards Guidance* to scan all IT assets, including but not limited to: computers, servers, routers, databases, operating systems, application, etc., that store and process government information. Provide scan reports to HHS/ FDA upon request. The contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

vi. **Vulnerability Management** - Contractors must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with the *FDA Information Security and Privacy Protection (IS2P)* policy and *HHS Policy for Vulnerability Management*. Automated tools must be compliant with NIST-specified SCAP standards for vulnerability identification and management. The contractor must maintain a capability to provide security vulnerability scanning

information for 100% of IT assets using SCAP-compliant automated tools and report to the agency at least monthly.

vii. **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and FDA patch management policy timeframes.

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

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

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

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

ii. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of

information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

- 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.

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

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

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

i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FDA encryption standard and current FIPS 140 validation certificate from the NIST CMVP.

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

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

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

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

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

- Using FDA-approved Security Content Automation Protocol (SCAP)-validated tools with capabilities to scan its systems at least on a monthly basis and report the results of these scans to the CO and/or COR, Project Officer, and any other applicable designated POC.

f. **Rights to Data.** All contracts that require data to be produced, furnished, acquired, or used in meeting contract performance requirements, must contain terms that delineate the respective rights and obligations of the Government and the contractor regarding the use, reproduction, and disclosure of that data. Data rights clauses do not specify the type, quantity or quality of data that is to be delivered, but only the respective rights of the Government and the contractor regarding the use, disclosure, or reproduction of the data. Accordingly, the contract must specify the data to be delivered.

g. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements**. The Contractor (and/or any subcontractor) must secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:

i. Develop rules for suppliers' development methods, techniques, or practices;

ii. Use of secondary market components;

iii. Prohibit counterfeit products;

iv. Dispose and/or retain elements such as components, data, or intellectual property securely;

v. Ensure adequate supply of components;

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

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

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

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

x. Prohibit the use of covered telecommunications and video surveillance equipment or services.

11. Confidentiality and Nondisclosure of Information

Any information provided to the contractor 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 or entity 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 shall be under the supervision of the Contractor. Each Contractor employee 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 can be used only for that purpose and to the extent authorized herein. The information shall not be disclosed to any other entity without prior FDA approval.

Contractor Non-Disclosure Agreement (NDA). Each Contractor employee having access to non-public government information under this contract shall complete the FDA non-disclosure agreement (3398 Form) (see Attachment 1), as applicable. Contractor must submit FDA form 3398 Prior to samples being sent and/or contractor employee performing work on the contract. Contractor will have up to 20 calendar days to return FDA form 3398 to the FDA. Upon receipt of samples, the contractor shall perform the required proteomics analysis which shall be delivered within 30 calendar days from receipt of the government provided human plasma samples. All data will be provided to FDA in a Microsoft Excel spreadsheet via email or an internet site for downloading. The service company does not own the data (i.e., intellectual property). FDA is the owner of the data.

Sanitization of Government Files and Information. As part of contract closeout and at expiration of the contract, the Contractorshall provide all required documentation to the 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

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).

CONTRACT ADMINISTRATION

Contracting Officer's Representative (COR):

Contract Officer Representative (COR):
Karyn Howard

Technical Point of Contact (TPOC):
Mayumi Miller

The contact information for the FDA Contracting Officer is the following:

Ian Weiss
U.S. Food and Drug Administration
Office of Acquisitions and Grants Services
4041 Powder Mill Road, 5th floor
Beltsville, MD 20705
Email: Ian.Weiss@fda.hhs.gov
Telephone: (301)796-5782

The Contracting Officer is the only person with authority to act as agent of the Government under this contract. Only the Contracting Officer has authority to direct or negotiate any changes in the order, including modifying or extending the period of performance, changing the delivery schedule, and authorizing reimbursement to the Contractor for any costs incurred during the performance of their contracts.

The contact information for the FDA Contract Specialist is the following:

Sheila Brown
U.S. Food and Drug Administration
Office of Acquisitions and Grants Services
4041 Powder Mill Road, 5th floor
Beltsville, MD 20705
Telephone: (301) 796-0827
Email: Sheila.Brown1@fda.hhs.gov.

CONTRACT CLAUSES

HHSAR Clauses Incorporated by Reference
This order incorporates the following U.S. Department of Health and Human Services Acquisition Regulation (HHSAR) 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 the following website: http://www.hhs.gov/policies/hhsar/.

HHSAR Clause	Description	Date
352.203-70	Anti-lobbying	(Dec 2015)
352.215-70	Late proposals and revisions	(Dec 2015)
352.223-70	Safety and health	(Dec2015)
352.224-70	Privacy Act	(Dec 2015)
352.233-71	Litigation and claims	(Dec 2015)

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: www.acquisition.gov/far/index.html
52.202-1 Definitions (June 2020)
52.203-5 Covenant Against Contingent Fees (May 2014)
52.203-7 Anti-Kickback Procedures (June 2020)
52.212-4 Contract Terms and Conditions-Commercial Items (Dec 2022)
52.233-4 Applicable Law for Breach of Contract Claim (Oct 2004)

52.212-5 Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services (JUN 2023)

(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) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).

(6) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(7) 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:

[*Contracting Officer check as appropriate*.]

__ (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. 4655).

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

_X_ (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).

_X_ (8) 52.204-27, Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

_X_ (9) 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).

__ (10) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018) (41 U.S.C. 2313).

__ (11) [Reserved].

__ (12) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (OCT 2022) (15 U.S.C. 657a).

__ (13) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (OCT 2022) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

__ (14) [Reserved]

__ (15)

(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.

__ (16)

(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.

__ (17) 52.219-8, Utilization of Small Business Concerns (OCT 2022) (15 U.S.C. 637(d)(2) and (3)).

__ (18)

(i) 52.219-9, Small Business Subcontracting Plan (OCT 2022) (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.

__ (19)

(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.

_X_ (20) 52.219-14, Limitations on Subcontracting (OCT 2022) (15 U.S.C. 637s).

__ (21) 52.219-16, Liquidated Damages—Subcontracting Plan (SEP 2021) (15 U.S.C. 637(d)(4)(F)(i)).

_X_ (22) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (OCT 2022) (15 U.S.C. 657f).

__ (23)

(i) 52.219-28, Post Award Small Business Program Rerepresentation (MAR 2023)(15 U.S.C. 632(a)(2)).

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

__ (24) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (OCT 2022) (15 U.S.C. 637(m)).

__ (25) 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 (OCT 2022) (15 U.S.C. 637(m)).

__ (26) 52.219-32, Orders Issued Directly Under Small Business Reserves (MAR 2020) (15 U.S.C. 644(r)).

_X_ (27) 52.219-33, Nonmanufacturer Rule (SEP 2021) (15U.S.C. 637(a)(17)).

_X_ (28) 52.222-3, Convict Labor (JUN 2003) (E.O.11755).

__ (29) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (DEC 2022) (E.O.13126).

X__ (30) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

__ (31)

X(i) 52.222-26, Equal Opportunity (SEP 2016) (E.O.11246).

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

_X_ (32) (i) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

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

_X_ (33) (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.

__ (34) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).

__ (35) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

__ (36)

(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).

__ (37) 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.)

__ (38)

(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.)

__ (39) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O. 13693).

__ (40) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).

__ (41)

(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.

__ (42)

(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.

__ (43) 52.223-15, Energy Efficiency in Energy-Consuming Products (MAY 2020) (42 U.S.C. 8259b).

__ (44)

(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.

__ (45) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (JUN 2020) (E.O. 13513).

__ (46) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).

__ (47) 52.223-21, Foams (Jun2016) (E.O. 13693).

__ (48) (i) 52.224-3 Privacy Training (JAN 2017) (5 U.S.C. 552 a).

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

_X_ (49) (i) 52.225-1, Buy American-Supplies (OCT 2022) (41 U.S.C. chapter 83).

__ (ii) Alternate I (OCT 2022) of 52.225-1.

__ (50) (i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (DEC 2022) (19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, 19 U.S.C. chapter 29 (sections 4501-4732), Public Law 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 [Reserved].

__ (iii) Alternate II (DEC 2022) of 52.225-3.

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

__ (v) Alternate IV (Oct 2022) of 52.225-3.

__ (51) 52.225-5, Trade Agreements (DEC 2022) (19 U.S.C. 2501, *et seq*., 19 U.S.C. 3301 note).

__ (52) 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).

__ (53) 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. Subtitle A, Part V, Subpart G Note).

__ (54) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

__ (55) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov2007) (42 U.S.C. 5150).

__ (56) 52.229-12, Tax on Certain Foreign Procurements (FEB 2021).

__ (57) 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. 3805).

__ (58) 52.232-30, Installment Payments for Commercial Products and Commercial Services (NOV 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

_X_ (59) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (OCT2018) (31 U.S.C. 3332).

__ (60) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

_X_ (61) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

__ (62) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

__ (63) 52.242-5, Payments to Small Business Subcontractors (JAN 2017) (15 U.S.C. 637(d)(13)).

__ (64)

(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:

[*Contracting Officer check as appropriate.*]

__ (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).

__ (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) 52.204-27, Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

(vi) 52.219-8, Utilization of Small Business Concerns (OCT 2022) (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.

(vii) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(viii) 52.222-26, Equal Opportunity (SEP 2015) (E.O.11246).

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

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

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

(xii) 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.

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

(xiv)

(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).

(xv) 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).

(xvi) 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).

(xvii) 52.222-54, Employment Eligibility Verification (MAY 2022) (E.O. 12989).

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

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

(xx)

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

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

(xxi) 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. Subtitle A, Part V, Subpart G Note).

(xxii) 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.

(xxiii) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.

(xxiv) 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)

Alternate I (FEB 2000). As prescribed in 12.301 (b)(4)(i), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".

Alternate II (JUN 2023). As prescribed in 12.301 (b)(4)(ii), substitute the following paragraphs (d)(1) and (e)(1) for paragraphs (d)(1) and (e)(1) of the basic clause as follows:

(d)(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8 G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to—

(i) Examine any of the Contractor's or any subcontractors' records that pertain to, and involve transactions relating to, this contract; and

(ii) Interview any officer or employee regarding such transactions.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), and (c), of this clause, the Contractor is not required to flow down any FAR clause in a subcontract for commercial products or commercial services, other than—

(i) *Paragraph (d) of this clause*. This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (d)(1)(ii) does not flow down; and

(ii) *Those clauses listed in this paragraph (e)(1)*. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

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

(B) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5).

(C) 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).

(D) 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).

(E) 52.204-27, Prohibition on a ByteDance Covered Application (JUN 2023) (Section 102 of Division R of Pub. L. 117-328).

(F) 52.219-8, Utilization of Small Business Concerns (OCT 2022) (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.

(G) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(H) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

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

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

(K) 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.

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

(M) __ *(1)* 52.222-50, Combating Trafficking in Persons (NOV 2021) (22 U.S.C. chapter 78 and E.O 13627).

__ *(2)* Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(N) 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).

(O) 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).

(P) 52.222-54, Employment Eligibility Verification (MAY 2022) (Executive Order 12989).

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

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

(S)__ *(1)* 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

__ *(2)* Alternate I (JAN 2017) of 52.224-3.

(T) 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. Subtitle A, Part V, Subpart G Note).

(U) 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.

(V) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.

(W) 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.

52.204-27 Prohibition on a ByteDance Covered Application.

As prescribed in 4.2203(c), insert the following clause:

PROHIBITION ON A BYTEDANCE COVERED APPLICATION (JUN 2023)

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

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) 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; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

(b) *Prohibition*. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on executive agency information technology, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the Contracting Officer provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) *Subcontracts*. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

(End of clause)

FAR 52.227-14, RIGHTS IN DATA-GENERAL

HHSAR 352.239-74: Information and Communication Technology (ICT) Accessibility (DEC 2015)

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

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

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

- Must meet WCAG 2.0 A and AA
- E101.2 Equivalent Facilitation (Appendix A, Application and Scoping Requirements)
- E203 Access to Functionality (Appendix A, Application and Scoping Requirements)
- E204 Functional Performance Criteria (Appendix A, Application and Scoping Requirements)
- E205 Electronic Content (Appendix A, Application and Scoping Requirements)
- E208 Support Documentation and Services (Appendix A, Application and Scoping Requirements)
- Chapter 6 Support Documentation and Services (Appendix C, Functional Performance Criteria and Technical Requirements)
- 302 Functional Performance Criteria (Appendix C, Functional Performance Criteria and Technical Requirements)
- Electronic content must be accessible to HHS acceptance criteria. Checklist for various formats are available at https://www.hhs.gov/web/section-508/making-files-accessible/index.html, or from the Section 508 Coordinator listed at https://www.hhs.gov/web/section-508/additional-resources/section-508-contacts/index.html. Materials that are final items for delivery should be accompanied by the appropriate checklist, except upon approval of the Contracting Officer or Representative.

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

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

(End of clause)

1. The following clauses are incorporated into the contract:

a. 352.232-71 Electronic Submission of Payment Requests (FEB 2022)

(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 identified in FAR 32.905(b), “Content of Invoices” and the applicable Payment clause included in this contract.

(b) Except as provided in paragraph (c) of this clause, the Contractor shall 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) The Contractor may submit payment requests using other than IPP only when the Contracting Officer authorizes alternate procedures in writing in accordance with HHS procedures.

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

(END OF CLAUSE)

b. 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 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.

a. 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).

b. Invoices that include cost-reimbursement Line Items must be submitted in a format showing expenditures for that month, as well as contract cumulative amounts.

At a minimum the following cost information shall be included, in addition to supporting documentation to substantiate costs incurred.

- Direct Labor - include all persons, listing the person's name, title, number of hours worked, hourly rate, the total cost per person and a total amount for this category;

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

c. 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.
(END OF CLAUSE)

INSTRUCTIONS TO THE OFFEROR

RESPONSE DATES

Offers in response to this solicitation shall be due no later than Friday, August 16, 2024, 3:30PM Eastern Standard Time and must be emailed to Sheila.Brown1@fda.hhs.gov. Questions are due no later than Monday, August 12, 2024, by 3:30 pm and must be emailed to Sheila.Brown1@fda.hhs.gov.

Instructions

Note: The Government reserves the right to evaluate quotes and make awards without discussions. Therefore, the Offeror's initial proposal shall contain the Offeror's best terms from a cost/price and technical standpoint. However, the Government may conduct discussions if the Contracting Officer determines they are necessary. Offeror are requested to demonstrate their expertise through a written quote. Quotes shall be separated into two (2) Volumes (Volume 1 – Technical Quotation, Volume 2 – Business Quotation as shown in the following table:

Please submit the following information for FDA's review:

Evaluation Factors for Award

Basis for Award

The Government will award a contract resulting from this solicitation to the responsible quoter as a fixed-price contract on the lowest price technically acceptable (LPTA) evaluation method. Award will be made on the basis of the lowest evaluated price meeting or exceeding the requirements of the solicitation, which specified in Section 4.0 Requirements and 5.0 Deliverables. The Quoter's initial quotation shall contain the Quoter's best terms from a price standpoint. Failure to demonstrate meeting any of the requirements will result in a rating of technically unacceptable and will not be considered for award. The FDA will also evaluate the fairness and price reasonableness of the total proposed pricing submitted.

Evaluation Criteria

The following factors shall be used to evaluate quotes:

- Total price. (Volume 2)
- Technical features meeting/exceeding requirements stated in Section 4.0 Requirements and 5.0 Deliverables. (Volume 1)
- Statement indicates that deliverables are meeting Section 508 compliance requirements. (Volume 1)

The Government will evaluate for compliance with the solicitation, assigning an "Acceptable" or "Unacceptable" rating for each factor:

The Offeror shall submit a written, comprehensive and executable narrative demonstrating that it possesses a full understanding of the Center for Veterinary Medicine/Office of Applied Science/Division of Applied Veterinary Research program requirements detailed in the Statement of Work (SOW) for whole genome sequencing and the relevant experience to execute all tasks and sub-tasks as identified.

> **Acceptable**: The Offeror demonstrates that the RFP requirements have been analyzed, evaluated, and synthesized into proposed approaches, plans, or techniques that, when implemented, shall result in adequate performance. The proposal has modest strengths. The weaknesses in the proposal are offset by the strengths. .**Unacceptable**: The Offeror demonstrates a superficial, incomplete, or incorrect understanding of the RFP requirements, resulting in proposed approaches, plans, or techniques that are deficient and shall result in poor performance when implemented. The proposal has few strengths. The proposal has significant weaknesses and/or many minor weaknesses that are not offset by strengths

Note: The Government is not responsible for locating or securing any information which is not identified in the quote. To ensure information is available, the offeror shall furnish as part of the quote, all descriptive materials necessary for the Government to unequivocally determine the services meet the technical requirements.

FDA is not responsible for any costs incurred in preparing a quotation responding to this Request for Quotation.