IDIQ STATEMENT OF WORK (SOW) FOR FOOD APPLICATIONS REGULATORY MANAGEMENT (FARM) & IT INTERFACING SYSTEMS
SOLICTATION #75F40126R00042
Amendment #1

1. Description/Specification

1.1. Background

The FDA is responsible for protecting public health by assuring the safety, effectiveness, and security of human and veterinary drugs, biological products, medical devices, cosmetics, the nation's food supply, and other products. The FDA regulates more than $1 trillion of consumer goods, representing about 25% of U.S. consumer expenditures. The Agency's optimal performance delivers significant public health and economic benefits by speeding innovations to market, ensuring access to accurate, science-based information, and coordinating with international organizations to investigate potential health risks, respond to emerging diseases, and address global public health challenges.

The Human Foods Program (HFP) oversees all FDA activities related to food safety and nutrition under the Deputy Commissioner of Human Foods. The HFP's mission is to ensure that food is a source of wellness for all U.S. consumers through science-based approaches to prevent foodborne illness, reduce diet-related chronic disease, and ensure chemicals in food are safe. The FDA's HFP - Office of Food Chemical Safety, Dietary Supplements and Innovation (OFCSDSI) operates multiple integrated IT systems to support its regulatory oversight of food chemicals and dietary supplements, including the Food Applications Regulatory Management (FARM), the Chemical Evaluation and Risk Estimation System (CERES), the Toxicology Reports and Analysis Management (TRAM) system, the Scientific Terminology and Regulatory Information (STARI), and the Warp Intelligent Learning Engine (WILEE). These systems provide robust data access, visualization capabilities, and system integration required to fulfill the office's scientific assessment and regulatory compliance mission.

The FARM system, initiated in 1995, supports premarket and post market safety review of petitions and notifications received from regulated industry. The system currently supports staff across HFP, including OFCSDSI, HFP-OFCSDSI-OPMA, HFP-OFCSDSI-ODSP, HFP-OFCSDSI-OPMAS, HFP-OFCSDSI-Innovative Foods Staff (IFS), Nutrition Center of Excellence (NCE)-Office of Nutrition and Food Labeling (ONFL) and Office of Critical Foods (NCE-OCF). Beyond HFP, FARM also supports the Office of Chief Scientist, Office of Cosmetics and Colors (OCAC), the Center for Veterinary Medicine (CVM)'s Ingredient Safety Team, Division of Animal Feeds, and scientific reviewers in the Center for Drug Evaluation and Research (CDER). FARM serves as the primary system for HFP reviewers to access and review industry submissions and conduct analysis with regards to chemical, toxicological, and environmental analysis and other issues, regarding specific ingredients, manage correspondence and Electronic Freedom of Information (EFOI) requests, and archive HFP historical files.

For OFCSDFI, the submissions/petitions evaluated include the following:
Food Additive Petitions (FAPs), Color Additive Petitions (CAPs), Generally Recognized as Safe Notices (GRNs), Food Contact Notifications (FCNs), Biotechnology Consultations (BNFs), New Protein Consultations (NPCs), Infant Formula Notifications (IFNs), Notifications for Food Allergens (NFAs), Petitions for Food Allergens (PFAs), Citizen Petitions (CZPs), Cell Culture Consultation (CCC), Cell Culture Ingredients (CCI), and Post-Market food safety assessments.

For the OFCSDSI-Office of Dietary Supplement Programs (ODSP), the submissions/petitions reviewed include the following:
New Dietary Ingredient Notifications (NDIs) and Structure Function Claims (SFCs).

For the Nutrition Center of Excellence - Office Nutrition, Food Labeling and (NCE-ONFL), the submissions/petitions evaluated include the following:
Citizen Petitions (CZPs) and Health Claims (HC).

In addition to providing information technology support to the scientific review of submissions, the FARM System is used to support critical regulatory functions for processing and documenting agency actions pertaining to pre-submission meetings, correspondences and requests for information sent to OFCSDFI, OFCSDFI-ODSP, OFCSDSI-OPMAS, OFCSDSI-OPMA, OFCSDSI-Innovative Foods (IFS), NCE-ONFL and OCS-OCAC such as: Prenotification Consultations, Prepetition Consultations, and Freedom of Information Act (FOIA) responses, Correspondence to OCS-OCAC, and Inquiries/Correspondence for NCE-ONFL.

The purpose of this ID/IQ is to establish a contracting vehicle for operations and maintenance and IT development services to support the mission of the various program areas. Successful offerors must demonstrate capability to work in a complex, multi-system environment where IT solutions directly support critical regulatory functions. The contractor will be expected to adapt to varying program area needs while maintaining system reliability and supporting FDA's public health mission.

Table 1. Recent submission data stored in the FARM system (2015 to 2025).

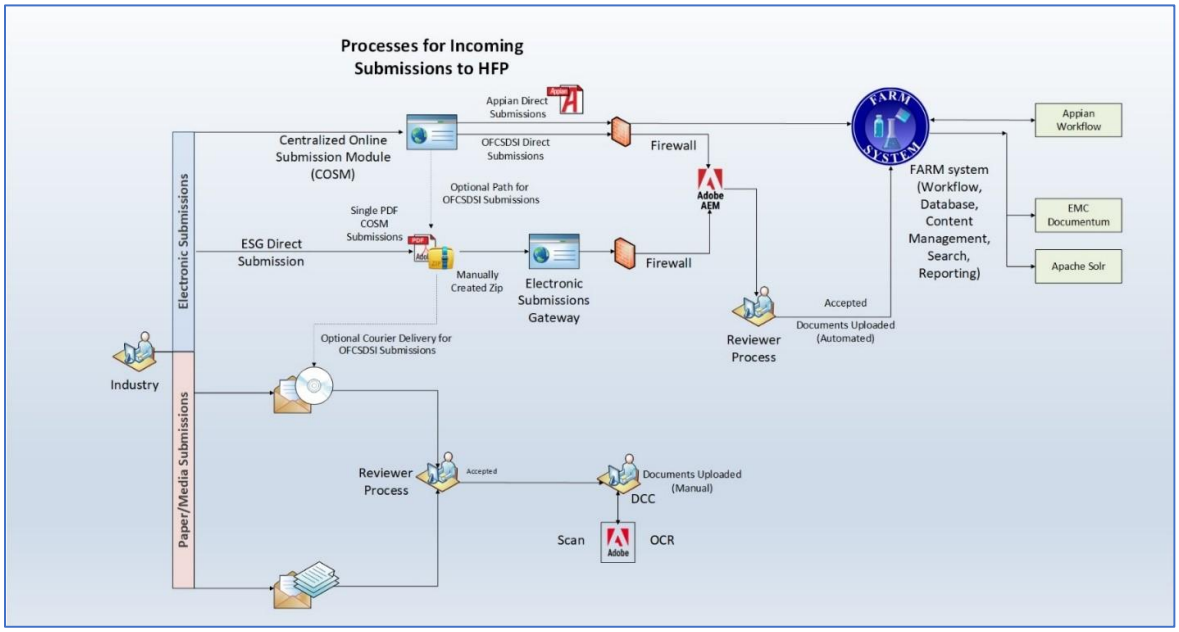
Submission Type	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
BNF	5	6	6	6	4	5	9	6	2	6
COR	126	98	103	31	18	180	357	427	442	275
FCN	113	122	97	79	82	4	74	67	76	77
EFOIA / FOI	207	205	232	280	235	266	234	264	316	276
GRN	73	64	85	72	86	58	82	49	52	53
GNF		33	35	33	21	37	28	28	24	13
GMT		0	1	0	1	0	0	0	0	1
NDI	0	0	0	2	65	57	56	51	71	85
PETITION	8	5	6	3	6	6	5	7	12	6
PNC	187	174	174	157	131	143	151	157	160	182
NPC	1	0	0	0	0	0	1	0	1	0
IFN		18	30	29	20	44	49	24	23	36
PMR		3	5	3	5	6	3	3	15	9
CZP -OFCSDSI (CZP)		15	0	0	1	4	0	5	0	4
OCZ-OFCSDSI-ODSP (OCZ)				0	0	0	0	0	0	0
COR-OFCSDSI-ODSP (CORDS)				167	459	180	272	366	168	58

SFC-OFCSDSI-ODSP				44	1432	1634	1482	1861	2542	2409
TOR				2	5	6	2	1	0	2
FALCPA				39	72	0	66	2	0	0
GBFP				105	8	72	110	78	100	82
GRAS				6	4	95	110	77	76	67

1.2. Technical Background

Human Foods Program (HFP) has iteratively upgraded the FARM System to its current configuration, an integrated system that supports online submission, content management, search/retrieval, workflows, account management, reporting, forms management, and indexing activities.

Exhibit 1 - FARM Features



FARM supporting software stack is provided in Table 2.

Table 2. Current FARM System technology stack

FARM Component / Software	FARM Component Software Version
Input/PDF Forms Management	Adobe Experience Manager (AEM) 6.5
Application Server	Oracle WebLogic 14C (14.1.2.0), Java jdk-21_linux-x64 jdk-21.0.8
Java JDK/JRE	Java JDK version 21.0.8 2025-07-15 LTS
Java J2EE	Jakarta EE 11
Spring Boot	2.7.18
Log4j	2.25.3

Apache PDF Box	2.0.4
Hibernate	5.6.15. Final (FARM Web); 5.6.15. Final (FARM API)
Jersey	2.35
Single Sign On (SSO)	Oracle SSO 14c
DB Storage	Oracle RDS 19c (Version 19.18.0.0.0)
Search	Apache Solr 9.10.1 (Zookeeper 3.9.4)
Content Management System	Documentum 24.4
Appian/Workflow	Appian 25.4
FARM Web Application UI	PrimeFaces 11.0.0
Business Object Reports	SAP BusinessObjects BI Platform 4.3 Sp4 Patch3
Electronic Submissions	MOVEit/file transfer version 14.1
COSM Internet UI Management	Angular 17.3.12, JWT 0.7.0, Angular Material 17.3.10, Bootstrap 5.3.8, Prime NG 17.18.15
Apache Kafka	2.13-4.1.0
Kafdrop	4.2.1
Swagger	5.17.14

1.3. Objectives & Scope

The purpose of this IDIQ Statement of Work is to obtain business and information technology support services (ITSS) for on-going operations and maintenance (O&M) and IT system development support using the current and enhanced infrastructure to various HFP IT systems.
As a direct result of contract performance, the FDA aims to achieve the following key outcomes:

- Management of the IT configuration, security requirements, upgrades and programming of software processes associated with the front-end processing of submissions and the back end integrating with the FARM system and other HFP interfacing systems.
- Optimize the FARM system online submission, content management, searching, workflow processes towards Intelligent Business Management (support content creation, review and authorization, categorization, reusability, storage and archiving, and retrieval of data) and reporting needs of HFP.
- Improve data quality, data profiling, governance and data integration between the FARM system data and other FDA data sets to facilitate the search and retrieval and sharing of information
- Improve information reporting capabilities across various data resources to support multiple FDA program areas

The contract encompasses the full range of Information technology services including online submission processing, content management, search management, database administration, customizations and process automation of workflows and reports, performance tuning and monitoring, system administration, help desk support, end-user training, infrastructure configuration, Enterprise Performance LifeCycle (EPLC), and security documentation management, and user account administration for the FARM system and other HFP IT systems.

1.3.1. Task Area 1 – Project Management (Firm Fixed Price)

The Contractor shall provide project management oversight the scope, schedule, quality, and cost are properly monitored and controlled throughout the duration of the contract.

Specifically, the Contractor PM shall perform these project management activities described in the following sections:

1.3.1.1. Meetings

The Contractor PM shall participate in the regular status meetings, technical and process improvement meetings. The Contractor PM shall prepare meeting agendas, minutes, issues, risks and action items with clear ownership, deadlines, and completion status to ensure accountability and follow-through.

1.3.1.2. Project Management Plan (PMP)

For the task orders released under this contract, the Contractor shall provide task order level PMP to establish control, management, monitoring and notification mechanisms, ensuring that contracted tasks stay on track and important milestones and performance measures are met. For each task order, the Contractor shall prepare a detailed Management Plan describing the technical approach to be employed for successful project execution. This plan must outline organizational resources that will be allocated to the task, including personnel assignments, and any specialized capabilities needed to fulfill the contract requirements. The Management Plan shall include robust risk management strategies, and other management controls that will be implemented to meet the cost, performance and schedule requirements throughout the entire duration of task order execution. These controls must demonstrate how the Contractor will proactively identify, assess, and mitigate potential risks while maintaining adherence to established budgets, performance standards, and delivery timelines. The plan serves as the foundational document that guides all project activities and ensures accountability at every phase of the work.

The Contractor shall provide monthly status reports on all awarded task orders and their progress to the IDIQ Task Order Contracting Officer Representative (COR). These reports are critical for maintaining transparency and ensuring effective oversight of contract performance throughout the project lifecycle. Within the first thirty (30) days after the contract award, the Government and the Contractor will collaborate to design and agree upon a standard reporting format that includes consistency and completeness of information to facilitate efficient review and analysis of project status. The agreed-upon reporting format shall include the following information at a minimum:

- Status and progress of tasks, providing clear visibility into completed work and upcoming activities
- Cost and schedule variances, highlighting any deviations from planned budgets and timelines along with explanatory details
- Significant risks to scheduled deliverables and comprehensive plans to mitigate them, ensuring proactive risk management
- Progress against service level metrics, demonstrating adherence to established performance standards and
- Recommendations for changes or additional activities to ensure that the tasks support progress on the overall contract objectives, enabling informed decision-making and timely course corrections when necessary to maintain project success and contract compliance.

In addition to progress reporting, the Contractor shall be proactive in informing the designated government Project Managers and Contracting Officer Representatives of any issues, problems and recommendations that should be addressed in order for the overall effective accomplishment of task order goals. Recommendations for actions that need to be taken by FDA staff, or other Contractors, shall be clearly defined and communicated to the responsible party and the FDA, and have identified dates for completion.

1.3.1.3. Reporting & Documentation

Weekly/Monthly/Annual Progress Reports: The Contractor PM shall submit Weekly, Monthly and Annual Reports and Project Schedule updates

1.3.1.4. EPLC Support & Documentation

The Contractor PM shall follow the FDA Enterprise Performance LiveCycle (EPLC) process and EPLC artifacts/deliverables

1.3.1.5. Release Management

The Contractor PM shall document the underlying software components and follow release management

1.3.2. Task Area 2 – Operations & Maintenance Support (Firm Fixed Price)

The Contractor shall perform technical upgrades and refreshes as directed, required and/or mandated by the FDA. The contractor will work with multiple HFP IT systems and interfaces to provide continuous IT solution support on a wide range of operations and maintenance services. For instance, FDA security classifies the FARM as a 'Mission Critical' system with a 24/7 operational requirement, excluding planned outages.

Representative activities under this task area may include:

- Provide user production support (such as FARM Helpdesk), user training and responses to Data Calls
- Coordinate, plan, develop, test, and implement all releases (major, minor, and emergency) following FDA EPLC standards with the FDA data center and Cloud environment contractors. Fix defects and perform minor enhancements (less than 200 hours for each enhancement), and incorporate them into releases
- Develop all documentation for EPLC intake processes and save all documents pertaining to the requirements, technical documents, user manuals, online help guides, etc., in the FDA document repository
- Implement infrastructure configuration and increase the scalability of system servers, keep the updated software stack within two versions of the latest release and perform annual operational analysis, by incorporating feedback from users of the IT systems
- Implement mandated security scan, such as Continuity of Operations (COOP) and Information Systems Contingency Plan (ISCP) exercise events that require Contractor support to meet all security requirements.
- Provide maintenance and database support for the FARM system

1.3.3. Task Area 3 – Information Technology System Development (Labor Hour)

The contractor will work on HFP IT systems and interfaces to perform on the development, modernization and enhancements (DME) tasks on a wide range of IT modernization services. The specific IT system development tasks will provide details about the IT systems to be changed or modified to substantively improve their capability or performance. Representative activities under this task area may include:

- Perform planning, analyzing and gathering requirements:

  - Analyze existing business processes, scenarios, activities, architecture, and information flow
  - Perform impact analysis scenarios and gap analysis activities to identify inefficiencies, redundancies, obsolescence, and technology gaps
- Design and develop IT application system per the requirements
  - Provide business and technology roadmaps to include blueprints, to-be business processes, information flow and data flow diagram, conceptual, data models, and system architectures that will transform the current state to the designed future state of business processes, web application and systems
- Test and Implement IT application system per the requirements into production

1.3.3.1. Create New or Enhance Workflows in Appian Cloud

The FARM System provides information management tools for Agency reviewers and is the key enabler of the electronic document review process and expedites the ingredient safety review process and subsequent safety decision-making effort to maximize productivity. Currently, FARM has 26 workflows:

- Collect new requirements, design, develop and implement enhancements to the existing workflows for HFP offices of Pre-Market Additive Safety, Post-Market and Assessment, Dietary Supplement Programs, Nutrition and Food Labeling and the Office of Cosmetics and Colors and other offices.
- Collaborate with the agency to implement AI-based Regulatory Review processes such as using FDA Elsa, Modernizing and Accelerating Regulatory Submissions tool (MARS) to embed AI into the workflow

1.3.3.2. Streamline Regulatory Review with AI-Enhanced Workflow Automation

- AI-Enhanced Review Automation: Implement AI and LLM tools (e.g., MARS, Elsa) within FARM Appian workflows to automate document processing, data extraction, classification, validation, preliminary assessments, and reporting, freeing scientific reviewers to focus on high-value safety evaluations.
- Decision Support & Standardization: Leverage historical data, external scientific databases, and AI recommendations to provide preliminary review synopses, reviewer assignments, standardized language suggestions, and flag inconsistencies against prior agency positions, ensuring regulatory consistency, rigor, and optimized workflow processes across HFP.
- Proof of Concept, Metrics, and Documentation: Deliver tested, agentic AI workflows with minimal human intervention; integrate with FDA-approved platforms (Appian, HALO-Databricks, consolidated data lakes) for intelligent routing and predictive analytics; demonstrate measurable reductions in administrative burden and increased reviewer time on scientific analysis; provide comprehensive system documentation, validation protocols, training materials, user guides, and feedback mechanisms to support adoption and continuous improvement.

1.3.3.3. Centralized Online Submission Module (COSM)

- Enhance COSM capabilities, collect, document, and validate technical and functional requirements; optimize system performance; implement monitoring and alerting; and establish standardized submission categorization and validation rules to improve system functionality and user experience.

- Support FDA IT consolidation initiatives by planning, designing, and implementing new user management requirements through the integration of COSM's web-facing interface functionalities with FDA's Identity, Confidentiality, Access, and Management (ICAM) public-facing systems and downstream systems, while ensuring the continuity of business operations.

1.3.3.4. Findability Enhancement of Regulatory Submission Data

- Enhanced Regulatory Data Access: Upgrade the interface for HFP and associated offices to improve findability and aggregation of regulatory and food safety information from internal and external FDA databases, including Harmonized Analytics Lifecycle Operations (HALO) data bricks. Enable scientists to access historical and current data efficiently for both premarket and post market reviews.
- Integration: Implement advanced search capabilities, including Boolean and proximity operators, improved sorting, enhanced metadata, document organization, and duplicate reduction. Integrate FDA AI tools to support intelligent search, document summarization, data extraction, similarity analysis, and regulatory precedent identification, leveraging MARS tool and HALO consolidated data.
- FARM Expansion, User Interface, and Training: Expand FARM search to support new submission types, substances, documents, COSM inquiries, and user notifications. Deliver a user-friendly interface with contextual search enhancements, downloadable search results, and integrated short tutorials. Provide comprehensive user guides and training materials to maximize adoption of advanced search and AI-powered features.

1.3.3.5. Integration with Interfacing Systems

- Enhance the integration of FARM with interfacing FDA IT systems such as EASE, TRAM/CERES, STARI, G-SRS, HFP-DW, and WILEE to enable seamless data exchange and interoperability
- Develop and implement integration interfaces to support bi-directional data flow between FARM components and external FDA systems
- Establish standardized data exchange protocols and APIs to facilitate real-time communication with interfacing systems
- Validate and test system integrations to ensure data accuracy, security, and compliance with FDA IT standards across all connected platforms

1.3.3.6. Development of Other HFP IT Systems

1.3.3.6.1. Perform Planning, Analyzing, and Gathering Requirements

1.3.3.6.2. Design and Develop per the requirements

1.3.3.6.3. Test and Implement per the requirements to release into production

1.3.4. Task Area 4 – Transition-In & Transition-Out (Firm Fixed Price~~Labor Hour~~)

1.3.4.1. Transition- In Support (Optional)

The Contractor shall provide Transition-In support in order to provide an orderly transition from the incumbent Contractor to the successor Contractor. The successor Contractor shall work toward the

Government's goal of ensuring minimal disruption to the current system and operational activities.

Working with the incumbent Contractor and the COR, the successor Contractor shall develop a plan to take over ongoing work from the incumbent Contractor as required in the Task Orders released under this IDIQ.

Representative activities may include:

- Develop a Transition-In plan,
- Participate in Transition-In meetings,
- Conduct and coordinating all on-boarding activities with the Government and obtaining secure badging for team personnel,
- Ensure staff identified as key personnel are available to work with Subject Matter Experts (SME) from the Government and the incumbent Contractor immediately after IDIQ Task Order awards,
- Engage in regularly scheduled meetings.

1.3.4.2. Transition-Out Support (Optional)

As tasked, the Contractor shall facilitate the transition of contracted FARM related activities and services to the Federal Government or to a follow-on Contractor at the end of the contract period of performance.

Representative activities under this task area may include:

- Provide the FDA with current versions of all systems and user documentation;
- Provide FDA all licensing and renewal information, asset management records, software documentation, and training materials;
- Provide FDA with a current inventory of all Government-owned assets used by the Contractor along with full support in the reconciliation of this inventory;
- Provide FDA with current versions of all CONOPS, operational procedures, standard operating procedures, guidelines, performance reports, specifications for hardware and software, and other pertinent information needed to continue the services being performed by the Contractor;
- Provide "shadowing" and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by the Contractor;
- Provide full source code sets (not COTS source code) with configuration management information; and,
- Provide up to date EPLC and program/project management documents.

2. Inspection & Acceptance

The FDA Contracting Officers Representative (COR) shall, in accordance with FAR 52.212-4, perform inspection and acceptance of all the services. The FDA COR will inspect and accept the services, documents, and materials provided to ensure they meet the requirements outlined in the contract. The FDA COR will accept goods, reports, and services only if they conform to all terms and conditions to the contract. Specific requirements for inspection and acceptance will be designated at the task order level. Acceptance shall be communicated within thirty (30) calendar days of receipt in writing.

3. Deliveries or Performance

The quoter or applicant shall submit all electronic documents for Microsoft Office suite products without the use of "macros". When submitting proposals via email, DO NOT include .exe, .mso, or any other executable file types that could potentially trigger email security protections (i.e. email blocks, quarantine). If the offeror or applicant submits documents that contain macros, macro referenced files, and/or executable files, the Government will not be able to view or open such documents and the submission will be considered non-responsive to the solicitation. No additional time will be given to a offeror or applicant to correct the document submission and the Government will not inform the offeror or applicant that their submission is non-responsive prior to award. It is the offerors or applicant's responsibility to ensure all electronic documents are submitted without the use of macros.
Deliverables shall be specified in the task orders issued under this contract. Deliverable products shall be reviewed, validated, and tested as appropriate to ensure that they meet applicable/specified standards, policy, business requirements and quality measures.
Draft versions of the contract level Program Management Plan (PMP) shall be submitted with the Offeror's proposal. Final versions of the PMP shall be delivered within thirty (30) days of contract award. When approved by the IDIQ COR, the Contractor shall operate under the PMP.

3.1. Period of Performance

In accordance with FAR 16.504(a)(4)(i), the anticipated period of performance of this IDIQ is sixty (60) months (five (5) years), as follows:

Ordering Period I: Twelve (12) months
Ordering Period II: Twelve (12) months
Ordering Period III: Twelve (12) months
Ordering Period IV: Twelve (12) months
Ordering Period V: Twelve (12) months

Individual periods of performance will be identified within each individual task order. Task orders may be issued up to the final day of this IDIQ, and the IDIQ shall remain in force to allow for the completion of all issued task orders (See FAR 52.216-22). The following constraints apply to the period of performance for task orders:

1. Individual task orders may not exceed five (5) years (inclusive of option periods).
2. Individual task orders may perform up to five (5) years (inclusive of options) beyond the expiration of this IDIQ, so long as the IDIQ maximum (inclusive of Ordering Periods I-V) is not exceeded.

In accordance with FAR 52.216-22, any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order.

3.2. Federal Holidays

Recognized Federal Holidays – The Contractor is not required to provide on-site services on the following days that are Federal Holidays or on any other day designated as a Federal holiday for the Washington, DC area (unless otherwise specified in the Task Orders):

New Year's Day	Martin Luther King's Birthday
President's Day	Memorial Day
Independence Day	Labor Day
Juneteenth National Independence Day	Veterans' Day
Columbus Day	Christmas Day

Thanksgiving Day

Inclement Weather – The Contractor is not required to provide on-site service on days when the Federal Government is closed due to inclement weather. The Contractor is required to follow, as a minimum, other directives issued by the U.S. Office of Personnel Management or other such official for late arrivals due to inclement weather (unless otherwise specified in the Task Orders).
In the event the Federal Government is closed by order of the President of the United States or the U.S. Office of Personnel Management for any reason, or the agency, the center or the building is closed for administrative or safety reasons, the Contractor will follow directives issued by responsible officials concerning reporting for work.
Each task order will contain instructions on what to do on those days when the Contractor is not permitted to report for work on-site because of a closure as determined above.

3.3. Place of Performance

The primary place of performance will be the FDA facilities within the Washington DC metropolitan area. Specific locations will be specified in each individual Task Order. Alternate locations may be approved on a Task Order basis. The contractor must use the BPA's **Government site rates** for authorized remote work; work not located at a contractor-owned facility.

Due to FDA-wide limited space availability, the Contractor may be expected to perform most contract development activities off-site, at the Contractor's proposed location. This can be near the Food and Drug Administration HFP, CPK2, 4300 River Road, University Station, College Park, MD, or it can be on/via Contractor's existing office spaces.
On-site meetings, supports and operations shall be performed at 4300 River Road, College Park, MD 20740 or other local FDA locations. Other contract-related technical works may be performed off-site via Virtual Private Network (VPN) using FDA-issued laptops, personal identity verification (PIV) cards (badges) and appropriate network accounts. The Contractor shall be responsible for providing internet access so Contractor-assigned computers can connect to the FDA network via VPN.
The Contractor may be required to move frequently while working at the various campuses. The Contractor may be required to utilize conference rooms, hoteling space, common areas, libraries, cafeterias, existing offices, or other shared space at the campus. The Contractors will need to be extremely mobile with no expectation of occupying the same work area for an extended period. Additional requirements may also be specified within each task order.

3.4. Travel

Travel costs within the Washington DC metropolitan area will not be reimbursed. Travel performed for personal convenience or daily travel to and from work at the Contractor's facility or local Government facility within the Washington DC metro region shall not be reimbursed hereunder. "Local" is defined under this term as the travel destination located within the Washington DC metro region. Travel outside of the Washington DC metropolitan area shall be conducted in strict accordance with the Federal Travel Regulations (FTR) and FAR 31.205-46. Any travel by the Contractor shall be conducted by the direction of the Government and must have written approval by the COR prior to booking and conducting travel. Costs associated with approved travel shall be reimbursed at actual cost, or by established Government per diems, whichever is less. Travel costs exceeding rates and per diems established under Federal Travel Regulations (FTR) are prohibited from reimbursement without written Contracting Officer approval prior to the associated travel being conducted. Prior to booking or conducting Government-

direct travel, the Contractor shall provide a written request for travel to the COR and CO. The Contractor's request for travel shall be in writing and contain the dates, locations and estimated costs of the travel. The Contractor shall then coordinate specific travel arrangements with the COR and must obtain advance, written COR approval for the travel to be conducted. The Contractor shall, to the maximum extent practicable, minimize overall travel costs by taking advantage of discounted airfare rates and other travel-related expenses available through advance purchase. Prior to changing and/or cancelling any travel that will incur cancellation fees, the Contractor shall notify the COR in writing of the total amount of the fees associated with Government-directed travel changes and/or cancellations. The Contractor shall consider and purchase reimbursable tickets when it is more beneficial to the Government.

3.5. Other Direct Costs (ODC)

Since ODCs are identified and acquired at the order level, the Contracting Officer is responsible for making a fair and reasonable price determination for all ODCs. To support the price reasonableness of ODCs, the contractor shall obtain quotes for each ODC item in accordance with the FAR procedures for that value of the ODCs included in the quote. The quotes must be submitted to the Government for concurrence of the Program Office and the Contracting Officer. The quotes shall be maintained by the contractor in the contractor's files and are subject to audit. The contractor may apply indirect costs, as a fixed amount, such as G&A and material handling costs and shall indicate the indirect cost rates applicable to the order. Fee, profit, and overhead may not be applied. All indirect costs must be sufficiently explained. If ODC's are required in an order in conjunction with services, the ODCs will have its own line item.

4. Contract Administration Data

4.1. Contract Type

This is anticipated to be a single-award Indefinite Delivery-Indefinite Quantity (IDIQ) contract. Authorized order types under this contract are: Firm Fixed Price (FFP) and Labor-Hour (LH), or a combination thereof.

4.2. Contract Value

See FAR 52.216-19 for individual task order limitations.

4.2.1. IDIQ Minimum

In accordance with FAR 16.504-1(b) the minimum guarantee for this IDIQ contract $1,000.00, which will be obligated to the IDIQ at the time of IDIQ award or will be obligated to a task order issued concurrently at the time of IDIQ award.

4.2.2. IDIQ Maximum

In accordance with FAR 16.504-1(c), the maximum aggregate dollar value of all task orders awarded over the entire period of performance of all single-award IDIQs combined shall not exceed the IDIQ ceiling amount of $25,000,000.00.

4.3. Government Points of Contact

The following individuals service as the Government points of contact for the IDIQ. Additional and/or different Government points of contact may be identified at the individual task order level. Unless otherwise specified, submit IDIQ deliverables to all Government points of contact listed below.

4.3.1. IDIQ Contracting Officer (CO)

Peter Lee
Peter.Lee@fda.hhs.gov
240-402-4287

The Contracting Officer (CO) identified above has responsibility for ensuring the performance of all necessary actions for effective contracting; ensuring compliance with the terms of the contract and safeguarding the interests of the United States in its contractual relationships. The CO is the only individual who has the authority to enter into, administer, or terminate this contract and is the only person authorized to approve changes to any of the requirements under this contract, and notwithstanding any provision contained elsewhere in this contract, this authority remains solely with the CO.
No statement, whether oral or written, by anyone other than the Contracting Officer, shall be interpreted as modifying the terms and conditions of this Task Order. It is the Contractor's responsibility to contact the CO immediately if there is even the appearance of any technical direction that is or may be outside the scope of the contract. The Government will not reimburse the Contractor for any work not authorized by the CO.

4.3.2. IDIQ Contract Specialist (CS)

Brian Wodzisz
Brian.Wodzisz@fda.hhs.gov
301-796-7376

4.3.3. IDIQ Contracting Officers Representative (COR)

To be determined @ time of award

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

4.4. Government Furnished Property/Information

GFP/GFI will be provided at the task order level. In general, the FDA will provide laptops Identity Verification (PIV) cards (badges) and appropriate network accounts. The Government Project Manager shall provide information and access to subject matter experts in both the business and technical areas as necessary. Independently, and not as an agent of the Government, the Contractor shall furnish the necessary services, personnel, materials, equipment, and facilities, not otherwise provided by the Government, as needed to perform this contract. The Contractor is responsible for all costs related to

making the property available for use, such as payment of all transportation, installation or rehabilitation costs

4.5. Ordering Procedures

In accordance with FAR 16.504-1, the Government will use the following procedures in issuing orders. In accordance with FAR 52.216-18, all task orders are subject to the terms and conditions of this contract. In the event of conflict between a task order and this contract, the contract shall control.

4.5.1. Placement of Orders

Individual orders shall be placed under this IDIQ in accordance with the procedures of FAR 16.505 and FAR 52.216-18.
In accordance with FAR 16.504-1, this IDIQ is available for use agency-wide and any FDA CO is authorized to issue orders.
A Request for Task Order Proposal (RFTOP) will typically be issued via email to the Contractor's email address.
In accordance with FAR 16.505(a)(2), individual orders will clearly describe all services to be performed or supplies to be delivered so the full cost or price for the performance of the work can be established when the order is placed. Orders shall be within the scope, issued within the period of performance, and be within the maximum value of the contract.
In accordance with FAR 16.505(a)(2), individual orders will clearly describe all services to be performed or supplies to be delivered so the full cost or price for the performance of the work can be established when the order is placed. In accordance with FAR 16.505(a)(7), orders placed under this indefinite-delivery contract will contain the following information:

(i) Date of order.
(ii) Contract number and order number.
(iii) For supplies and services, line item number, subline item number (if applicable), description, quantity, and unit price or estimated cost and fee (as applicable). The corresponding line item number and subline item number from the base contract shall also be included.
(iv) Delivery or performance schedule.
(v) Place of delivery or performance (including consignee).
(vi) Any packaging, packing, and shipping instructions.
(vii) Accounting and appropriation data.
(viii) Method of payment and payment office, if not specified in the contract (see 32.1110(e)).
(ix) North American Industry Classification System code (see 19.102(b)(3)). Any work that the Contractor undertakes prior to receiving a fully executed task order that has been signed by the CO (or the Contractor has received prior authorization to proceed from the CO) shall be at the Contractor’s risk.

4.5.2. Pricing of Orders

Proposals submitted in response to a RFTOP must use labor rates equal to or less than the established IDIQ Ordering Period labor rates listed in the IDIQ Price Schedule based on the date the work is actually performed. If a task order’s performance period crosses into new IDIQ Ordering Period rates, the Contractor may propose the next applicable IDIQ Ordering Period rates for that portion of the performance period. The Contractor may propose lower rates in response to a RFTOP. RFTOPs may include option periods in accordance with FAR clause 52.217-9.

The Contractor shall comply with FAR 52.212-4, Contract Terms and Conditions—Commercial Products and Commercial Services, with regard to fixed-prices for individual deliverables and FFP task orders. The total amount specified in FFP deliverables and task orders shall be fixed for the period of performance and shall not be subject to adjustment; except, as a result of a direct action or inaction by the Government, which delays the Contractor from completing the task within the time specified in the order.
The Contractor shall comply with FAR 52.212-4, Contract Terms and Conditions—Commercial Products and Commercial Services—Alternate I, with regard to the ceiling price for individual labor categories and LH task orders. LH task orders will include a ceiling price. If a task order's stated period of performance must be extended as a result of Government delay, the Contractor may request that the most current labor rates be used to price the work effort during the extended period for LH task orders.
The Contractor's pricing schedules for labor categories shall contain fully burdened hourly labor rates, including all wages, indirect costs, fringe benefits, overhead, general and administrative, and profit. Hourly rates apply to services at both Government and non-Government sites. By mutual agreement of the parties, additional labor categories may be added to this IDIQ contract to support the tasks of this contract.

4.6. Invoicing

The Contractor shall include the payment address, if it is different from that shown for the Contractor.

Specific invoicing instructions may be provided in each individual task order. Unless otherwise specified, the FDA invoicing procedures shall be in accordance with HHSAR 352.232-71, Electronic Submission of Payment Requests, and as follows:

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.

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

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

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

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

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

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

- invoice number, amount, & date submitted
- corresponding payment amount & date received
- total amount of all payments received to date under the subject contract or order
- 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)

4.7. Availability of Funds

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

5. Special Contract Requirements

Additional and/or specific special contract requirements

5.1. Section 508 Requirements

Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) requires Federal agencies to purchase information and communication technologies (ICT) that meet specific accessibility standards. This law helps to ensure that federal employees with disabilities have access to, and use of, the information and data they need to do their jobs. Furthermore, this law ensures that members of the public with disabilities have the ability to access government information and services.

There are three regulations addressing the requirements detailed in Section 508. The Section 508 technical and functional standards are codified at 36 CFR Part 1194 and may be accessed through the Access Board's Web site at http://www.access-board.gov. The second regulation issued to implement Section 508 is the Federal Acquisition Regulation (FAR). FAR Part 39.2 requires that agency acquisitions of information and communication technology (ICT) comply with the Access Board's standards. The entire FAR is found at Chapter 1 of the Code of Federal Register (CFR) Title 48, located at http://www.acquisition.gov. The FAR rule implementing Section 508 can be found at http://www.section508.gov. The third applicable regulation is the HHS Acquisition Regulation (HHSAR). Regardless of format, all Web content or communications materials produced for publication on or delivery via HHS Web sites - including text, audio or video - must conform to applicable Section 508 standards to allow federal employees and members of the public with disabilities to access information that is comparable to information provided to persons without disabilities. All contractors (including subcontractors) or consultants responsible for preparing or posting content intended for use on an HHS-funded or HHS-managed Web site must comply with applicable Section 508 accessibility standards, and

where applicable, those set forth in the referenced policy or standards documents below. Remediation of any materials that do not comply with the applicable provisions of 36 CFR Part 1194 as set forth in the SOW, shall be the responsibility of the contractor or consultant retained to produce the Web-suitable content or communications material.

Unless an agency exception to this requirement exists, the Contractor must conform to applicable Section 508 standards and must apply best practices associated with Section 508 compliance during the application design, development, and testing phases. The Contractor shall utilize FDA approved tools to verify the compliance with the Section 508 standards and ensure the delivery of the fully compliant products.

The following Section 508 standards apply to this Statement of Work (SOW):

- 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.

5.2. Security Requirements

A. <u>Baseline Security Requirements</u>

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:

Protect the:

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

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

- **Confidentiality:** [ ] Low [X] Moderate [ ] High
- **Integrity:** [ ] Low [X] Moderate [ ] High
- **Availability:** [ ] Low [X] 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 [ ] Yes 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

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.

program for official travel to any foreign country. Please see the FDA IS2P, *Appendix T Government Furnished Equipment for Foreign Travel*.

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.

B. 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.

C.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.

D. 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.

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.

E. Position Sensitivity Designations

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

F. 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.

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

H. Contract Initiation

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.

Procurements Involving Government Information Processed on GOCO or COCO Systems

1. Security Requirements for GOCO and COCO Resources

a. **Federal Policies.** The Contractor (and/or any subcontractor) must comply with applicable federal laws and HHS and FDA policies that include, but are not limited to, the *HHS*

Information Security and Privacy Protection (IS2P) policy; *FDA Information Security and Privacy Protection (IS2P) policy*; *Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, latest revision, *Security and Privacy Controls for Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, Departmental, and Agency policies.

b. **Assessment and Authorization (A&A)**. A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) must work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s): *[Within 30 days].* The Contractor must conduct the A&A requirements in accordance with *HHS IS2P/ FDA IS2P* NIST SP 800-37, *Guide for Applying the Risk Management Framework to Information Systems: A Security Life Cycle Approach* (latest revision), NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, and the NIST SP 800-53A (latest revision).

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.

- **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.

Cloud Services

1. HHS FedRAMP Privacy and Security Requirements The Contractor (and/or any subcontractor) must be responsible for the following privacy and security requirements:

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

i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *FDA Information Security and Privacy Protection (IS2P)* Policy, *HHS Information Security and Privacy Protection (IS2P)* policy and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor must also implement a set of additional controls identified by the agency when applicable.
ii. A security control assessment must be conducted by a FedRAMP third party assessment organization (3PAO) for the initial ATO and ***annually*** thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

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

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

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

2. Protection of Information in a Cloud Environment

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

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

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

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

i. Maintenance of links between records and metadata, and
ii. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

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

i. If the system involves the design, development, or operation of a Privacy Act system of records on individuals, the Contractor must comply with the Privacy Act requirements as follows:

Adhere to the information collection, use, sharing, maintenance, and other requirements detailed in the System of Records Notice(s) (SORN(s)) that is applicable to this contract: [FDA requiring activity insert SORN number if one exists. If there is no SORN, indicate that a SORN will be developed].

The design, development, or operation work the Contractor is to perform is: [FDA requiring activity insert description of design, development, and/or operation work; see definitions in the FAR at 24.101 - Definitions].
The disposition to be made of the Privacy Act records upon completion of contract performance is: [FDA requiring activity insert records disposition instructions the contractor and any subcontractor must follow upon completion of contract performance].

3. Assessment and Authorization (A&A) Process

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

i. In addition to the FedRAMP compliant ATO, the contractor must complete and maintain an agency A&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the FDA authorizing official (AO) prior to implementation of system and/or service being acquired.
ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO but should not use self-assessment. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.
iii. For all acquired cloud services, the A&A package must contain the following documentation: See the A&A package deliverables from Section 4 and/or deliverables mentioned in the FedRAMP Standard Contract Language available on the FedRAMP site. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS and FDA policies using FDA templates.

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

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

d. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A&A and continuous monitoring activities. All vulnerabilities and findings must be remediated, in accordance with timelines specified in the FDA POA&M Standard, from discovery: (1) critical vulnerabilities no later than ***fifteen (15) days*** and (2) high within **thirty (30) days** (3) medium within **ninety (60) days** and (4) low vulnerabilities no later ***than three hundred and sixty (90) days.*** In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA&M and mitigated within the designated timelines.

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

4. Reporting and Continuous Monitoring

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

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

i. Operating system, database, Web application, and network vulnerability scan results;
ii. Updated POA&Ms;
iii. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the FDA Owner or AO; and
iv. Any configuration changes to the system and/or system components or CSP's cloud environment, that may impact HHS/FDA's security posture. Changes to the configuration of

the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the agency.

5. Configuration Baseline

a. The contractor must certify that applications are fully functional and operate correctly as intended on systems using *Minimum Security Configuration Standards for FDA Information Technology Systems* and *HHS Minimum Security Configurations Standards Guidance*. The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved HHS and FDA configuration baseline.

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

6. Incident Reporting

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

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

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

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

- Company and point of contact name;

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

7. Media Transport

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

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

8. Boundary Protection: Trusted Internet Connections (TIC)

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

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

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

Security Deliverables

Deliverable Title/Description	Type	Due Date	POC
Roster	Electronic	Within *[10 business days]* of the effective date of this contract	COR
Contractor Employee Non-Disclosure Agreement (NDA)	Electronic	Prior to performing any work on behalf of HHS/FDA	COR
Assist in the completion of a PTA/PIA form	Electronic	Per timeline as specified by the FDA Privacy POCs. after contract award	COR
Copy of training records for all mandatory training	Electronic	In conjunction with contract award and annually thereafter or upon request	COR

Signed rules of behavior (ROB) for all employees	Electronic	Initiation of contract and at least annually thereafter	COR
Incident Report (as incidents or breaches occur)	Electronic	As soon as possible and without reasonable delay and no later than 1 hour of discovery	COR
Incident and Breach Response Plan	Electronic	Upon request from Government	COR
List of Personnel with defined roles and responsibilities	Electronic	Within a time directed by the COR that is before an employee begins working on this contract	COR
Off-boarding documentation, equipment and badge when leaving contract	Electronic	The last day that work is being performed after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.	COR
Background Investigation - Onboarding documentation when beginning contract.	Electronic	Prior to performing any work on behalf of HHS/FDA	COR
Certification of Sanitization of Government and Government Activity	Electronic	At contract expiration.	COR

Contractor Personnel Security Clearance Standards and Residency Requirements

1. BACKGROUND - The Office of the Assistant Secretary for Management and Budget, Department of Health and Human Services (DHHS), requires that Contractor employees (including subcontractors) who will be working in DHHS-owned or leased space and/or who will have access to DHHS equipment, and non-public privileged, proprietary, or trade secret information, must undergo a background investigation that results in a favorable determination.

Contractor employees who will work in DHHS-owned or leased space for less than thirty (30) days are considered visitors and are exempted from background investigation requirements; and therefore, will not be issued a Personal Identity Verification (PIV) Card. These contractor employees go through visitor screening each day and must be escorted at all time while in DHHS- owned or leased space.

2. GENERAL - The Contractor must submit the following items to the Contracting Officer's Representative (COR), within <u>five (5) business days</u> of commencement of work under this contract:

- A roster of contractor employee names, identifying Key Personnel and Tier designation(s);
- Confirmation all individual employee security information has been submitted properly; and
- "Contractor's Commitment to Protect Non-public Information Agreement" forms signed by each employee named in the roster.

Pursuant to HSPD-12, the Contractor must advise its prospective employees about the security and background requirements stated herein.
For any individual who does not obtain a favorable background investigation he/she must cease work on the contract immediately.

If a Contractor employee changes job responsibilities under this contract, the Contractor must notify the COR, and the Government will make a determination whether an additional security clearance is required.
In the event there are any proposed personnel changes in the Contractor's staffing roster previously submitted to the COR, the Contractor must submit an updated roster to the COR, along with a brief explanation for the change. In turn, the COR will initiate the procedures stated herein to ensure any new contractor employees obtain a PIV card in a timely manner – prior to that individual commencing work under the contract.

Note: If the proposed personnel change is for a position designated Key Personnel under the contract, a complete justification – along with a resume or curriculum vitae – must be submitted to the Contracting Officer and COR for review and approval. If approved, the Contracting Officer will execute a Contract Modification prior to that individual commencing work under the contract.

3. BACKGROUND INVESTIGATIONS - With the exception of costs associated with fingerprinting Contractor employees outside of the FDA Personnel Security Office, the Government will conduct all required background investigations at no cost to the Contractor. The cost of fingerprinting Contractor employees at any location other than the FDA Personnel Security Office will be borne by the Contractor. Employees who hold or have previously held a Government security clearance must advise the FDA Personnel Security Staff of the details of such clearance.

Note: Background investigations will be conducted by the Office of Personnel Management (OPM)

4. CONTRACT RISK DESIGNATION(S) - Contractor employees who will be in DHHS- owned or leased space for thirty (30) days or more must be able to obtain and shall obtain a PIV card pursuant to Homeland Security Presidential Directive-12 (HSPD-12) in order to access to DHHS-owned or leased property without an escort. (See Section 6 for details on the PIV Card process) However, in the event that work must commence before a security screening can be completed, contractor employees will be considered visitors, as described above, and allowed onto DHHS-owned or leased property, but must be escorted at all times.

All Contractor employees who undergo a background investigation are required to log onto the Office of Personnel Management's (OPM's) Electronic Questionnaire for Investigation Processing system (e-Qip) system. The FDA Personnel Security Specialist will provide access to the e-Qip as well as guidance as to which forms will be required. The forms required vary with the position risk designations for the contract.

All standard forms submitted to the FDA will be forwarded to the Office of Personnel Management (OPM) to initiate background investigations. The assigned FDA Personnel Security Specialist will resolve with the contractor employee any issues arising out of inaccurate or incomplete forms.

The Risk Designation(s) for this contract is/are Tier(s): 2

There are three (3) potential position risk designations, which are:

- Non-Sensitive Low Risk (Tier 1) - Positions which involve the lowest degree of adverse impact on the efficiency of the Agency. The forms set forth by the FDA Personnel Security Specialist are required for Non-Sensitive Low Risk Positions.
- Sensitive Moderate Risk (Tier 2) or Sensitive High Risk (Tier 4) - Public Trust Positions - Positions in which the incumbent's actions or inaction could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs.

In order to access the e-QIP system, Contractor employees must provide the appropriate FDA Personnel Security Specialist with the following information: (a) full name; (b) position title; (c) social security number; (d) date of birth; (e) place of birth; (f) email address; and (g) phone number. This information will be provided on the e-Qip form that will be electronically sent to the employee. The FDA Personnel Security Specialist will use this information to enter each Contractor employee into the e-QIP system. Once this is done, each Contractor employee will receive an email that contains a web link to access the e-QIP system, as well as instructions and additional forms needed to initiate the background investigation.
A Contractor's failure to comply with the e-QIP processing guidelines will result in that Contractor's employees being denied access to FDA property until all security processing has been completed. Furthermore, any such noncompliance may detrimentally impact Contractor performance, Contractor performance evaluations, rights and remedies available at law and equity retained by the Government.

5. PERSONAL IDENTITY VERIFICATION (PIV) CARDS - All PIV Cards (and any other type of Government-issued Access Card) shall remain the property of the Federal Government. At any time, if a Contractor employee is terminated or otherwise ceases work under the contract, or no longer requires a PIV Card for contract performance purposes, the Contractor must collect the individual's PIV card and immediately notify FDA Personnel Security Staff in writing, with copies to the respective COR and Contracting Officer. The Contractor must immediately return the PIV Card(s) to the COR.
Because PIV Cards, like other Government-issued Access Cards are Government property, Contractors and Contractor Employees are hereby placed on notice that any abuse, destruction, defacement, unauthorized transfer or withholding (i.e., failure to return to the Government) may be punishable to the greatest extent at law.
Unauthorized possession of a PIV Card, or any other type of Government-issued Access Card, and/or willfully allowing any other person to have or to use your Access Card, is prohibited and can be criminally prosecuted under 18 U.S.C. §§ 499 and 70I, which prohibit photographing or otherwise reproducing or possessing HHS identification cards in an unauthorized manner, under penalty of fine, imprisonment, or both. Wrongdoers may also be held financially responsible for any/all civil and equitable remedies – to include, but not limited to, damages for any pecuniary loss suffered by the Government as a result of any of the above-listed actions or failure to act.

6. PIV CARD PROCESS - The COR will sponsor Contractor employees on the Form HHS 745 and HHS Smart Card Management System (SCMS) for the purpose of obtaining an FDA PIV Card. In

order to obtain a PIV card, a Contractor employee must receive a favorable FBI fingerprint return and complete required security forms. The FDA Personnel Security Specialist will provide the Contractor employee(s) direction for scheduling fingerprinting appointments at the FDA location or other approved location.

During a fingerprint appointment, each contractor employee must present two (2) forms of identification in order to receive his or her PIV Card. One form of identification must be a government-issued photo identification document. Acceptable forms of identification are listed in
Appendix A, provided below. An individual who receives an unfavorable report may appeal that finding by submitting a written request to the FDA Personnel Security Specialist.
Required background investigations may include, but are not limited to:

- Review of prior Government/military personnel records;
- Review of FBI records and fingerprint files;
- Searches of credit bureaus;
- Personal interviews; and
- Written inquiries covering the subject's background.

7. RESIDENCY REQUIREMENTS FOR FOREIGN NATIONALS - Under the requirements for Homeland Security Presidential Directive-12 (HSPD-12), OPM can complete a background investigation only for persons who have resided in the U.S. for a total of at least three (3) of the past five (5). The residency requirements apply only to foreign nationals. **If any prospective foreign national contractor/subcontractor employee does not meet the residency requirements, he/she cannot qualify for a PIV Card under HSPD-12**.

8. NON-PUBLIC DATA PROTECTION - The Contractor must protect the privacy of all information reported by or about Contractor employees and protect against unauthorized disclosure.

***Upon a favorable fingerprint return, the Contractor will be notified to return to the Badging and Credentialing Office for their building pass.**

Food and Drug Administration Badging and Credentialing Office
8:00 a.m. – 11:00 a.m. and 1:00 p.m. – 3:00 p.m.,
Eastern Time 10903 New Hampshire Avenue
Building 32, Room 1205 Silver Spring, MD 20993
No appointment necessary Telephone:
(301) 796-4000

Appendix A

LIST A Documents that Establish Both Identity and Employment Authorization	OR	LIST B Documents that Establish Identity	AND	LIST C Documents that Establish Employment Authorization
1. U.S. Passport or U.S. Passport Card		1. Driver's license or ID card issued by a State or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		1. A Social Security Account Number card, unless the card includes one of the following restrictions: (1) NOT VALID FOR EMPLOYMENT (2) VALID FOR WORK ONLY WITH INS AUTHORIZATION (3) VALID FOR WORK ONLY WITH DHS AUTHORIZATION
2. Permanent Resident Card or Alien Registration Receipt Card (Form I-551)		2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address		2. Certification of report of birth issued by the Department of State (Forms DS-1350, FS-545, FS-240)
3. Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa		3. School ID card with a photograph		3. Original or certified copy of birth certificate issued by a State, county, municipal authority, or territory of the United States bearing an official seal
4. Employment Authorization Document that contains a photograph (Form I-766)		4. Voter's registration card		4. Native American tribal document
5. For a nonimmigrant alien authorized to work for a specific employer because of his or her status: a. Foreign passport; and b. Form I-94 or Form I-94A that has the following: (1) The same name as the passport; and (2) An endorsement of the alien's nonimmigrant status as long as that period of endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form.		5. U.S. Military card or draft record		5. U.S. Citizen ID Card (Form I-197)
		6. Military dependent's ID card		6. Identification Card for Use of Resident Citizen in the United States (Form I-179)
		7. U.S. Coast Guard Merchant Mariner Card		7. Employment authorization document issued by the Department of Homeland Security
		8. Native American tribal document		
		9. Driver's license issued by a Canadian government authority		
		For persons under age 18 who are unable to present a document listed above:		
6. Passport from the Federated States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the United States and the FSM or RMI		10. School record or report card		
		11. Clinic, doctor, or hospital record		
		12. Day-care or nursery school record		

6. List of Attachments

6.1. SOL_RFP_75F40126R00042
6.2. Attachment_1_IDIQ_SOW
6.3. Attachment_2_TO1_SOW_OM
6.4. Attachment_A_Pricing Schedule and LCAT
6.5. Attachment_B_Appendix_1