Food and Drug Administration (FDA) - BlinkID PDF417 B2B Annual license Maintenance
Center for Tobacco Programs (FDA/CTP)

"Brand Name or Equal Solution"
FDA-20-SOL-1227378

Statement of Work (SOW)

1.0 Background

MicroBlink's BlinkID PDF417 B2B is a tool that enables users to scan, extract data from ID's, passports or driver licenses within a few seconds and translate that data into an existing application. The technology uses a mobile device's camera to read the PDF417 barcode from a U.S drivers licenses. The Center for Tobacco Products, Office of Compliance and Enforcement's (OCE) FDA Age Calculator mobile application is utilized by tobacco retailers and their clerks to scan the U.S. federal, state, or territorial government-issued driver's license, U.S. state or territorial department of motor vehicle photo identification, and U.S. military photo identification (hereinafter U.S. government-issued photo ID) of tobacco customers. Retailers are required by law to verify the age of the consumer purchasing tobacco products and confirm if they met the legal age (18 years old) requirement so they may legally purchase regulated tobacco products under federal law. In order for CTP to maintain access to the product we are required to annually purchase the MicroBlink PDF417 B2B Annual License Fee which includes product support, maintenance, and upgrades as done in year's past. CTP has utilized this technology for the past 2 years.

2.0 Objective

The objective is to procure one (1) B2B License Fee which shall provide continued access to the MicroBlink PDF 417 B2B tool.

3.0 Business Need

Currently CTP OCE FDA Mobile Age Calculator app for Apple iOS (iPhone & iPad) and Android OS requires MicroBlinkID PDF 417 B2B plugins to enable mobile devices to read driver license, state IDs and Military ID. If CTP does not procure MicroBlinkID PDF 417 B2B licenses on or before September 28th, 2019 this application will cease functioning. CTP has explored other application solutions, but no other solutions exist in the market place at this time.

4.0 Product Description

The vendor shall provide the MicroBlinkID 417 B2B Licenses for unlimited users. The license shall include support and maintenance. The maintenance shall be included in the MicroBlinkID PDF 417-B2B software license.

The solution must meet the following salient characteristics:

5.0 Salient Characteristics and Functional Specifications

The contractor shall provide software licenses required to perform all the following functions:

1. Native plugins for mission critical barcode scanner.
2. Plugins should work in any mobile operating system, i.e. Apple's iOS and Android.
3. Plugins support.
4. Plugins shall allow users to scan any Federal or State Issued REAL-ID license with barcode.

6.0 Section 508 ICT Accessibility Requirements Statement

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)
- 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 http://508.hhs.gov/, 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.

Appropriate Scoping Requirement from Appendix A

- E207 Software (Appendix A, Application and Scoping Requirements)
- E208 Support Documentation and Services (Appendix A, Application and Scoping Requirements)

Appropriate Technical Performance and Technical Requirement from Appendix C

- Chapter 5 Software (Appendix C, Functional Performance Criteria and Technical Requirements)
- Chapter 6 Support Documentation and Services (Appendix C, Functional Performance Criteria and Technical Requirements)

6.0 FDA IT Security Requirements

A. BASELINE SECURITY REQUIREMENTS

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

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

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

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

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

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

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

Management Center (SMC) within one (1) hour of discovery/detection in the event of an information security incident.

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

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

4) **Information Security Categorization**. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, Appendix C, and based on information provided by the ISSO or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality: [ ] Low [X] Moderate [ ] High

Integrity: [ ] Low [X] Moderate [] High

Availability: [ ] Low [X] Moderate [ ] High

Overall Risk Level: [ ] Low [X] Moderate [ ] High

Based on information provided by the Privacy Office, system/data owner, or other privacy representative, it has been determined that this solicitation/contract involves:

[ ] No PII [X] Yes PII

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

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

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

a. marked appropriately;

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

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

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

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

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

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

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

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

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

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

*See **Appendix D** for baseline deliverables.*

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

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

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

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

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

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

11) **Contractor Non-Disclosure Agreement (NDA)**. Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the FDA non-disclosure agreement (3398 Form), as applicable. A copy of each signed

and witnessed NDA shall be submitted to the CO and/or COR prior to performing any work under this acquisition.

12) **Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)** – The Contractor shall assist the procuring activity representative, program office and the FDA SOP or designee with conducting a PTA for the information system and/or information handled under this contract to determine whether or not a full PIA needs to be completed.

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

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

B. TRAINING

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

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

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

and ***annually*** thereafter or upon request.

C. RULES OF BEHAVIOR

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

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

D. INCIDENT RESPONSE

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

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

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

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

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

2) NOT notify affected individuals unless so instructed by the Contracting Officer or designated

representative. If so instructed by the Contracting Officer or representative, the Contractor shall send FDA approved notifications to affected individuals as directed by FDA's SOP.

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

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

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

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

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

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

E. POSITION SENSITIVITY DESIGNATIONS

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

F. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-12

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

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

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

G. CONTRACT INITIATION AND EXPIRATION

1) **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor shall follow the FDA EPLC framework and methodology in accordance with the HHS Contract Closeout Guide (2012).

   HHS EA policies may be located here: https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-for-enterprise-architecture.html

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

3) **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation in accordance with FDA OAGS SMGs to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, Guidelines for Media Sanitization and FDA IS2P Appendix T: *Sanitization of Computer-Related Storage Media*

4) **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR as soon as it is known that an employee will stop working under this contract.

5) **Contractor Responsibilities Upon Physical Completion of the Contract**. The contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems)

acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or FDA policies.

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

H. RECORDS MANAGEMENT AND RETENTION

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

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

A. Privacy Act

It has been determined that this contract is subject to the Privacy Act of 1974, because this contract provides for the design, development, or operation of a system of records about individuals.

The System of Records Notice (SORN) that is applicable to this contract is: *[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]*.

I. SECURITY REQUIREMENTS FOR Government Owned/Contractor Operated(GOCO) AND Contractor Owned/Contractor Operated (COCO) RESOURCES

1) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *FDA Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and* Organizations; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

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

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

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

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

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

annually thereafter. **Security Assessment Plan/Report (SAP/SAR)** – due before the system is made available to standard users. The security assessment shall be conducted by FDA's team of security assessors, unless otherwise noted and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and FDA policies. The assessor will document the assessment results in the SAR.

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

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

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

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

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

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

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and FDA IS2P. The following are the minimum requirements for ISCM:

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

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

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

- **Vulnerability Management -** Use FDA-approved SCAP-compliant automated tools for authenticated

  scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS and FDA policy. Automated tools shall be compliant with NIST- specified SCAP standards for vulnerability identification and management. The

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

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

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

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

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

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

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

b. At any tier handling or accessing protected information, fully cooperate with all audits,

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

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

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

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

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

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

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

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

d. Validate the configuration settings after hardware and software installation, operation,

maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

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

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

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

f.

SECURITY REQUIREMENTS FOR Government Owned/Contractor Operated(GOCO) AND Contractor Owned/Contractor Operated (COCO) RESOURCES

6) **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *FDA Information Security and Privacy Policy (IS2P), Federal Information Security Modernization Act (FISMA) of 2014, (44 U.S.C. 101)*; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and* Organizations; Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Departmental policies.

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

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

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

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

- **System Security Plan (SSP)** – due a week prior to the start of the annual security assessment. The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, and other applicable NIST guidance as well as HHS and FDA policies and other guidance. The SSP shall be consistent with and detail the approach to IT security contained in the

Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system, as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost- effective security protection for a system.

The Contractor shall update the SSP at least ***annually*** thereafter. **Security Assessment Plan/Report (SAP/SAR)** – due before the system is made available to standard users. The security assessment shall be conducted by FDA's team of security assessors, unless otherwise noted and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and FDA policies. The assessor will document the assessment results in the SAR.

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

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

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

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

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

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

b. Information Security Continuous Monitoring. Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/or transmit government information, shall meet or exceed the information security continuous monitoring (ISCM) requirements in accordance with FISMA and NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and FDA IS2P. The following are the minimum requirements for ISCM:

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

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

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

- **Vulnerability Management -** Use FDA-approved SCAP-compliant automated tools for authenticated

  scans to scan information system(s) and detect any security vulnerabilities in all assets (computers, servers, routers, Web applications, databases, operating systems, etc.) that store and process government information. Contractors shall actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS and FDA policy. Automated tools shall be compliant with NIST- specified SCAP standards for vulnerability identification and management. The

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

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

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

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

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

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

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

b. At any tier handling or accessing protected information, fully cooperate with all audits,

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

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

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

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

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

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

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

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

d. Validate the configuration settings after hardware and software installation, operation,

maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and

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

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

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

CONTRACTOR PERSONNEL SECURITY CLEARANCE STANDARDS AND RESIDENCY REQUIREMENTS (OCTOBER 2017)

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 five (5) business days 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 - N/A):

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

- Non-Sensitive Low Risk (Tier – N/A) - 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 – N/A(Tier) or Sensitive High Risk (Tier – N/A) - 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

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

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		

7.00 Place of Performance

The task will be performed at FDA, 5001 Campus Drive, College Park, Maryland, 20740. Meetings and work sessions may be conducted at other FDA Offices in Rockville or Beltsville as necessary and shall be coordinated thru the FDA Contractor Officer Representative or designee. Work shall be conducted Monday through Friday, excluding federal holidays. Unless otherwise directed, the Contractor shall adhere to standard work hours, working no more than forty (40) hours per week, and observe all U.S. Government holidays. The on-site Contractor shall maintain continuous service during the hours at the facility identified above.

8.0 Period of Performance

12 Months

9.0 Government Point of Contact

Contracting Specialist/Officer
Jacquelyne Ngegba
301-796-6761
Jacquelyne.Ngegba@fda.hhs.gov

10.0 Contract Type
Firm Fixed Price

11.0 The following Clauses are applicable:

FAR Clauses:
52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

52.204-9 - Personal Identity Verification of Contractor Personnel (Jan 2011)

52.224-1 Privacy (Apr 1984)

52.232-18 Availability of Funds (Apr 1984)

52.245-1 Government Property (Jan 2017)

52.227-14 Rights in Data - General (May 2014)

52.244-6 Subcontracts for Commercial Items (Jan 2019).

HHSAR Clauses:

352.203-70 Anti-Lobbying (Dec 2015)

352.208-70 Printing and Duplication (Dec 2015)

352.222-70 Contractor Cooperation in Equal Employment Opportunity Investigations (Dec 2015)

352.224-70 Privacy Act (Dec 2015)

352.231-70 Salary Rate Limitation (Dec 2015)

352.237-75 Key Personnel (Dec 2015)

HHSAR Provision

352.239-73 Electronic Information and Technology Accessibility Notice

Instructions to Offeror's
A completed version of the chart below (or something substantially similar) shall be included in the quote. In addition to this pricing information, the Vendor shall provide product specifications for the specific items that are listed above.

CLIN	DESCRIPTION	MANUFACTURER/ PART NUMBER	UNITS	UNIT PRICE	TOTAL PRICE

Quoters' shall submit all applicable terms and conditions in full text as attachments, appendix, or exhibits.

Quoters' are advised that additional terms and conditions submitted with their quotations that are in conflict with the terms and conditions of this solicitation may be deemed as technically unacceptable and as such not be considered for award.

Quoters' shall submit Product Accessibility Templates (PAT) in full text with their quotations (attached). Additional PAT information can be found at: https://www.hhs.gov/web/section-508/contracting/index.html

Failure to submit a PAT may deemed a quote as technical unacceptable and as such not be considered for award.
Quoters' shall submit all assumptions in their quotation.

Quoters' shall notify the Contract Specialist/Contracting Officer immediately if this requirement is registered by a reseller with the Original Equipment Manufacturer (OEM).

Quoters' shall provide documentation of been an authorized reseller and/or servicing agent for the solution.

In order for a vendor proposal to be evaluated, the vendor must include, "Vendor Response to FDA Software Requirement", Excel spreadsheet with the vendor response to this requirement.

The vendor shall only complete all Green cells included in the, "Vendor Response to FDA Software Requirement", Excel spreadsheet.

Evaluation Criteria
All quotations will be evaluated on a Lowest Priced Technically Acceptable (LPTA) basis. The award will be made to the lowest price vendor who demonstrates that all requirements of the solicitation are met. Failure to demonstrate meeting any of the requirements or instructions will result in a rating of technically unacceptable and will not be considered for award. Incomplete quotations will not be considered for award.

The offeror or applicant shall submit all electronic documents for Microsoft Office suite products without the use of "macros". If the offeror or applicant submits documents that contain macros the Government will not be able to view or open such documents and the submission will be considered non-responsive to the solicitation. No additional time will be given to an offeror or applicant to correct the document submission and the Government will not inform the offeror or applicant that their submission is non-responsive prior to award. It is the offeror's or applicant's responsibility to ensure all electronic documents are submitted without the use of macros.