A. Baseline Security Requirements

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

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

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

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

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

b. Provide security for any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor on behalf of HHS 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.

c. Adopt and implement the policies, procedures, controls, and standards required by the HHS 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 HHS Information Security Program security requirements, outlined in the HHS Information Security and Privacy Policy (IS2P), by contacting the CO/COR or emailing fisma@hhs.gov.

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

3. Information Security Categorization. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories, Appendix C, and based on information provided by the ISSO, CISO, 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: [X] Low [ ] Moderate [ ] High
Overall Risk Level: [ ] Low [X] Moderate [ ] High

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

[ ] No PII [X] Yes PII

Personally Identifiable Information (PII). Per the Office of Management and Budget (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

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

    a. marked appropriately;

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

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

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

6. **Confidentiality and Nondisclosure of Information**. Any information provided to the contractor (and/or any subcontractor) by HHS or collected by the contractor on behalf of HHS 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 HHS 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 CDC policies. Unauthorized disclosure of information will be subject to the HHS/CDC 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 provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

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. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and OpDiv-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 have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR prior to performing any work on behalf of HHS.

    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 shall be provided to the COR upon request and at the conclusion of the contract.

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 CDC nondisclosure agreement. A copy of each signed and witnessed NDA shall be submitted to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

12. **Privacy Impact Assessment (PIA)** – The Contractor shall assist the CDC Senior Official for Privacy (SOP) or designee with conducting a PIA for the information system and/or information handled under this contract.

    a. The Contractor shall assist the CDC SOP or designee with completing a PIA for the system or information within prior to performing any work on behalf of HHS in accordance with HHS policy and OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.

    b. The Contractor shall assist the CDC SOP or designee in reviewing the PIA at least every **year** 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.

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 HHS/OpDiv 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 CDC 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 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 policy and the HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum.

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 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, and CDC Implementation of the HHS Rules of Behavior for Use of HHS Information Technology Resources.

2. All Contractor employees performing on the contract must read and adhere to the Rules of Behavior before accessing Department 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 OpDiv 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

The Contractor (and/or any subcontractor) shall respond to all alerts/Indicators of Compromise (IOCs) provided by CDC Computer Security Incident Response Team (CSIRT) 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 Federal Information Security Modernization Act (FISMA) as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The HHS Policy for IT Security and Privacy Incident Reporting and Response further defines a breach as "a suspected or confirmed incident involving PII".
In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) shall:

1. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract so as 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 CDC approved notifications to affected individuals within 30 days.

3. Report all suspected and confirmed information security and privacy incidents and breaches to the CDC Computer Security Incident Response Team (CSIRT) at 866-655-2245 and CSIRT@cdc.gov, COR, CO, OpDiv SOP (or his or her designee), 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**, and consistent with the applicable CDC 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, HHS and CDC 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.

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:

[ ] Level 6C: Sensitive - High Risk
[X] Level 5C: Sensitive -Moderate Risk

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 shall be submitted to the COR and/or CO within 14 of the effective date of this contract. Any revisions to the roster as a result of staffing changes shall be submitted within 14 of the change. 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 HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Guide (2012).

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 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.

4. **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and system ISSO within 14 days before an employee stops 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 CDC policies.

6. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the CDC Contractor Employee Separation Checklist when an employee terminates work under this contract within 1 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/CDC policies and shall not dispose of any records unless authorized by HHS/CDC.

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/CDC policies.

HHSAR "Privacy Act" clause, 352.224-70):
PII means 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. OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016). 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.

The E-Government Act of 2002 Section 208 (E-Government Act) and Office of Management and Budget (OMB) Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government of 2002, form the core of the Privacy Impact Assessment (PIA) requirement. Together, they state that a PIA is an assessment of how information is handled within certain electronic systems. Each PIA should consider: 1) Whether the system complies with legal, regulatory, and policy requirements related to privacy; 2) The risks and effects of how that system handles personally identifiable information (PII); and 3) How the system could be changed to mitigate potential privacy risks. The Department of Health and Human Service (HHS) has chosen to evaluate the privacy implications of all electronic systems regardless of whether the E-Government Act or OMB M-03-22 requires a PIA.

Privacy or Security Safeguards (FAR Clause 48 CFR § 52.239-1)

1. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

3. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

Confidential Information (HHSAR Clause 48 CFR § 352.224-71)

1. Confidential Information, as used in this clause, means information or data of a personal nature about an individual, or proprietary information or data submitted by or pertaining to an institution or organization.

2. Specific information or categories of information that the Government will furnish to the Contractor, or that the Contractor is expected to generate, which are confidential may be identified elsewhere in this contract. The Contracting Officer may modify this contract to identify Confidential Information from time to time during performance.

3. Confidential Information or records shall not be disclosed by the Contractor until:

a. Written advance notice of at least **45 days** shall be provided to the Contracting Officer of the Contractor's intent to release findings of studies or research, to which an agency response may be appropriate to protect the public interest or that of the agency.
b. For information provided by or on behalf of the government,
   i. The publication or dissemination of the following types of information are restricted under this contract: NONE
   ii. The reason(s) for restricting the types of information identified in subparagraph (i) is/are: None
c. Written advance notice of at least 45 days shall be provided to the Contracting Officer of the Contractor's intent to disseminate or publish information identified in subparagraph (2)(i). The contractor shall not disseminate or publish such information without the written consent of the Contracting Officer.
d. Whenever the Contractor is uncertain with deciding if information is confidential under this contract, the Contractor should consult with the Contracting Officer prior to any release, disclosure, dissemination, or publication of that information.

Privacy Threshold Analysis (PTA)[1] – due within 45 days after contract award

1. The Contractor shall assist the Senior Agency Official for Privacy (SAOP) (or his or her designee)[2] with conducting a PTA (using the Privacy Impact Assessment [PIA] form) for the information system and/or information collection project 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 the SAOP (or his or her designee) and other designated authorities with completing a PIA for the system or project within 30 days after completion of the PTA.
   b. The PIA shall be completed in accordance with HHS policy, OMB M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (https://www.whitehouse.gov/omb/memoranda_m03-22) and shall be revised at each milestone during the system development lifecycle (SDLC).
   c. PIAs must be reviewed at least **annually** and whenever a significant change is made to the information systems or when new PII is collected, that introduces new or increased privacy risks.

Deliverables:

Deliverable Title/Description	Due Date
Roster	Within 7 days of the effective date of this contract
Contractor Employee Non-Disclosure Agreement (NDA)	Prior to performing any work on behalf of HHS
Copy of training records for all mandatory training	In conjunction with contract award and annually thereafter or upon request
Signed ROB for all employees	Initiation of contract and at least annually thereafter
Incident and Breach Response Plan	Upon request from government
List of Personnel with defined roles and responsibilities	Within 7 days that is before an employee begins working on this contract.
Off-boarding documentation, equipment and badge when leaving contract	Within 7 days after the Government's final acceptance of the work under this contract, or in the event of a termination of the contract.
Onboarding documentation when beginning contract.	Prior to performing any work on behalf of HHS

I. Personnel Security Responsibilities

1. The Contractor, within **7 days** before an employee begins working on this contract, shall provide the COR and/or Contracting Officer, and Information System Security Officer (ISSO) the name, position title, e-mail address, and phone number of all contract employees working under the contract per the National Industrial Security Program Operating Manual (NISPOM) Section 2-200 (http://intranet.hhs.gov/security/ossi/documents/nispom.pdf), the HHS Contract Closeout Guide (2012)

(http://intranet.hhs.gov/abouthhs/contracts-grants-support/acquisition-policies-guidance/acquisitionworktools/contract-closeout-tableofcontents/), and the HHS Personnel Security & Suitability Policy, Section 7.6 (http://intranet.hhs.gov/security/ossi/documents/pssp.pdf).

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

3. If the employee is filling an existing position, the Contractor shall provide the name, position title and suitability determination level held by the former incumbent.

4. The Contractor shall notify the COR and/or Contracting Officer and system ISSO within 14 days before an employee stops working under this contract.

5. The Contractor shall provide the name, position title, and suitability determination level held by or pending for departing employees to the COR and/or Contracting Officer.

6. The Government will stop pending background investigations for employees that no longer work under this acquisition.

7. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the Contractor Employee Separation Checklist when a Contractor (and/or any subcontractor) employee terminates work under this contract. All documentation shall be made available to the COR and/or Contracting Officer upon request.

8. Within 5 days after the Government's final acceptance of the work under this contract, or upon termination of the contract, the Contractor shall return all identification badges to the Contracting Officer or designee.

J. Fingerprinting

1. All Contractor (including any subcontractor) employees must be fingerprinted before gaining access to HHS-controlled information systems in compliance with FAR Subpart 52.204-2 Security Requirements (including Alternate II) (https://www.acquisition.gov/?q=/browse/far/52).

2. To gain logical access to HHS-controlled information systems, contract employees working under the contract are subject to a fingerprint check.

3. If a Contractor (and/or any subcontractor) must appear at an HHS facility to be fingerprinted, any costs associated with getting to that facility are to be borne by the Contractor.

K. Background Investigations

1. All Contractor (including any subcontractor) personnel must complete a background investigation based on the position designation and type of investigation required as determined by the agency in compliance with FAR Part 52.222-54 -- Employment Eligibility Verification (https://www.acquisition.gov/?q=/browse/far/52) and FAR Subpart 22.18— Employment Eligibility Verification (https://www.acquisition.gov/?q=/browse/far/22).

2. At the time of solicitation, based upon information provided by the CO/COR, the Contracting Officer shall specify all known levels. If the position sensitivity levels are not known at that time, the Contracting Officer shall insert the words "To Be Determined at the Time of Award." However, the Contracting Officer must include the definitive position sensitivity levels in the awarded contract/order.

3. The personnel investigation procedures for Contractor personnel (and/or any subcontractor) require that the Contractor (and/or any subcontractor) prepare and submit background check/investigation forms based on the type of investigation required. The minimum Government investigation for a non-sensitive position is a National Agency Check and Inquiries

(NACI) with fingerprinting. More restricted positions – i.e., those above non-sensitive, require more extensive documentation and investigation.

i. The Contractor shall notify the CO/COR of its proposed personnel who will be subject to a background check/investigation.
ii. The Contractor shall notify the CO/COR whether any of its proposed personnel who will work under the contract have previously been the subject of national agency checks or background investigations.

4. Investigations are expansive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with the FAR section, Excusable Delays – see FAR 52.249-14, if applicable (https://www.acquisition.gov/sites/default/files/current/far/html/52_248_253.html).
   i. The Contractor shall ensure that the employees it proposes for work under this contract have a reasonable chance for approval.
5. The Government may investigate personnel at no cost to the Contractor. However, multiple investigations for the same position may, at the Contracting Officer's discretion, justify reduction(s) in the contract price of no more than the cost of the additional investigation(s).

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 on individuals.

1. Privacy Act Notification (FAR Clause 48 CFR § 52.224-1). The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of Section (i) of the Act may involve the imposition of criminal penalties.

2. Privacy Act (FAR Clause 48 CFR § 52.224-2). The Contractor agrees to –

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies –

   i. The systems of records;
   ii. The design, development, or operational work that the contractor is to perform.

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

   i. Include this clause, including this paragraph, in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
      - In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of Section (i) of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

c. "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

d. "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and

criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

e. e. "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

3. **Privacy Act (HHSAR Clause 48 CFR §352.224-70).** This contract requires the Contractor to perform one or more of the following: design; develop; or operate a Federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) (5 U.S.C. 552a(m)(1)) and applicable agency regulations.

a. The term system of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Violations of the Act by the Contractor and/or its employees may result in the imposition of criminal penalties (5 U.S.C. 552a(i)).

b. The Contractor shall ensure that each of its employees knows the prescribed rules of conduct in 45 CFR part 5b and that each employee is aware that he/she is subject to criminal penalties for violation of Section (i) of the Act to the same extent as Department of Health and Human Services employees. These provisions also apply to all subcontracts the Contractor awards under this contract which require the design, development or operation of the designated system(s) of records (5 U.S.C. 552a(m)(1)). The contract work statement:

i. Identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and
ii. Specifies the disposition to be made of such records upon completion of contract performance.
iii. Specifies the use of a disclosure statement (required by Section (e)(3) of the Privacy Act of 1974, as amended) to appear on documents used to obtain PII from individuals to be maintained in a Privacy Act System of Records (SORN).

The System of Records Notice (SORN) that is applicable to this contract is: Privacy Act System of Records Number 09-20-0147, Occupational Health Epidemiological Studies and EEOICPA Program Records.

The design, development, or operation work the Contractor is to perform are: Identify data relevant to reconstructing radiation doses and evaluating SEC petitions, claimant Communications, Dose estimation and reporting, prepare Special Exposure Cohort petition evaluations, and technical and program management support.

The disposition to be made of the Privacy Act records upon completion of contract performance are:

L. 1. Audit Record Retention

a. The Contractor (and/or any subcontractor) shall support a system in accordance with the requirement for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 (http://www.gpo.gov/fdsys/granule/CFR-2011-title36-vol3/CFR-2011-title36-vol3-sec1236-20) & 1236.22 (http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36:3.0.10.2.25) (ref. a), including but not limited to capabilities such as those identified in:
i. NARA Bulletin 2013-02, August 29, 2013, Guidance on a New Approach to Managing Email Records (https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html),
ii. ii NARA Bulletin 2010-05 September 08, 2010 (http://www.archives.gov/recordsmgmt/bulletins/2010/2010-05.html), Guidance on Managing Records in Cloud Computing Environments (ref 8).

These provide requirements for maintaining records to retain functionality and integrity throughout the records' full lifecycle including:
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.

B. Privacy Plan

The Contractor shall submit a plan with its technical proposal, in accordance with the HHS IS2P, that safeguards data and protects the confidentiality of PII (NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information, http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf and NIST SP 800-53, Revision 4,, Appendix J http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf); the plan shall:

- Verify the information categorization to ensure the identification of the PII requiring protection.
- Verify the existing risk assessment.
- Identify the Contractor's existing internal corporate policy that addresses the information protection requirements of the SOW.
- Verify the adequacy of the Contractor's existing internal corporate policy that addresses the information protection requirements of the SOW.
- Identify any revisions, or development, of an internal corporate policy to adequately address the information protection requirements of the SOW.
- For PII to be physically transported to or stored at a remote site, verify that the security and privacy controls of NIST Special Publication 800-53, latest version, involving the encryption of transported information will be implemented.
- When applicable, verify how the NIST Special Publication 800-53, latest version, security and privacy controls requiring authentication, virtual private network (VPN) connections and other technical safeguards will be implemented.
- When applicable, verify how the NIST Special Publication 800-53, latest version, security controls enforcing allowed downloading of PII will be implemented.
- Identify measures to ensure subcontractor compliance with safeguarding PII and security and privacy controls in the NIST 800-53.
- Be commensurate with the size and complexity of the contract requirements based on the System Categorization specified above in the subparagraph entitled Security Categories and Levels.
- Be evaluated by the Government for appropriateness and adequacy.

A. Security Requirements for GOCO and COCO Resources

1. **Federal Policies.** The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the HHS Information Security and Privacy Policy (IS2P), [no applicable OpDiv policy identified]; 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 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) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s): Due within 30 days after contract award. The Contractor shall conduct the SA&A requirements in accordance with HHS IS2P/HHS-OCIO, NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (latest revision).

   CDC 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 30 days after contract award to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package:

- **System Security Plan (SSP)** – due within 30 days after contract award. 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 NIOSH/DCAS 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 within 30 days after contract award. The security assessment shall be conducted by an independent assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and OpDiv policies. The assessor will document the assessment results in the SAR.

  Thereafter, the Contractor, in coordination with CDC shall assist in the assessment of the security controls and update the SAR at least **annually**.

- **Independent Assessment –** due within 30 days after contract award. The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the Security Authorization package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all "high" deficiencies before submitting the package to the Government for acceptance. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).

- **POA&M** – due within 30 days after contract award. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and OpDiv policies. All high-risk weaknesses must be mitigated within 2 days and all medium weaknesses must be mitigated within 7 days from the date the weaknesses are formally identified and documented. DCAS 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 documented 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, DCAS may require designated POAM 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 within 30 days after contract award. 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 OpDiv 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, Rev. 2, Electronic Authentication Guidelines.

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 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 HHS 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 independent third-party. In addition, review all relevant SA&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date DCAS provided.

- **Asset Management -** Using any available 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 HHS-owned information/data. It is anticipated that this inventory information will be required to be produced at least 30 days. 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 available 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 **monthly**. 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 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 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 agency specified timeframes. The contractor shall report status when the directed action has been completed.

- **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, 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.

   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; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO). The contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with HHS 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 HHS 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 and FIPS 140-2 encryption standards.

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

c. Maintain the latest operating system patch release and anti-virus software definitions;

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 security policies, including but not limited to:

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

- Using 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.

Data Protection. Current Federal government security guidance requires that sensitive government information that is stored on laptops and other portable computing devices shall be encrypted using Federal Information Processing Standard (FIPS)-140-2 validated encryption. The contractor shall provide the percentage of portable IT assets that are equipped with FIPS 140-2 validated encryption, to encrypt all sensitive government information, via a report on a **quarterly** basis. Additionally, ensure that all privacy controls are implemented and working as intended.

Remote Access. Current Federal government security guidance requires that two-factor authentication be implemented when remotely accessing sensitive government owned information/data on IT systems (both government owned and contractor owned systems). Additional Federal government security guidance when remotely accessing government owned information/data include the following: connections shall utilize FIPS-140-2 validated encryption; connections shall be capable of assessing and correcting system configurations upon connection; connections shall be capable of scanning for viruses and malware upon connection; connections shall prohibit split tunneling; and connections shall require timeout after **15 minutes** of inactivity. Each quarter, the contractor shall provide the following information about the contractor's remote access solutions to government owned sensitive information/data: percentage of current connections that allow connection using only a password; percentage of connections that require the use of a government provided personal identity verification (PIV) card as part of a two-factor solution; percentage of connections that require the use of other two- factor authentication solutions; percentage of connections that utilize FIPS-140-2 encryption; percentage of connections that assess and correct system configurations upon connection; percentage of connections that scan for viruses and malware upon connection; percentage of connections that prohibit split tunneling; and percentage of connections that require timeout after **15 minutes** of inactivity.

Standard for Security Configurations. The Contractor (and/or any subcontractor) shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS (http://intranet.hhs.gov/it/cybersecurity/enterprise_security/config_mgmt/).

M. Hardware Acquisitions

1. The Contractor (and/or any subcontractor) shall include Federal Information Processing Standard (FIPS) 201-compliant (https://www.idmanagement.gov/IDM/IDMFicamProductSearchPage) smart card readers (referred to as LACS Transparent Readers) with the purchase of servers, printers, desktops, and laptops; in compliance with FAR Part 12 – Acquisitions of Commercial Items (https://www.acquisition.gov/far/html/FARTOCP12.html) and FAR Subpart 4.13- Personal Identity Verification (https://www.acquisition.gov/sites/default/files/current/far/html/Subpart 4_13.html).

(**NOTE**: COs/CORs must consult the OMB M-16-02, "Improving the Acquisition and Management of Common Information Technology: Laptops and Desktops" https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-02.pdf) before procuring Desktop and laptop equipment.)

2. **Mobile Devices**. The contractor shall ensure that NIST 800-124, Rev. 1 Guidelines for Managing the Security of Mobile Devices in the Enterprise (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) is followed when using mobile devices that process or store HHS data.

N. Information Technology Application Design or Support

The Contractor (and/or any subcontractor) shall ensure IT applications designed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges per the HHSAR Subpart 352.239-70--Standard for Security Configurations.