NHLBI's *Learn More Breathe Better*®
2025-2026 Community Subcontract Program

Appendix A: Budget Template for NHLBI Partner Program for COPD Education Proposals

Please use this budget template to construct your project budget. You may expand this budget to add as many line items as needed.

1. Direct Expenses (materials, vendors, equipment, travel, etc.)

Item	Total Project Cost	Funding Requested for this subcontract	Funding from other sources*	Comments, explanation
SUBTOTAL, Direct Expenses				

2. Staffing and Personnel (labor)

Person, title Cost (hourly rate x hours)**	Total Project Cost	Funding Requested for this subcontract	Funding from other sources*	Comments, explanation
SUBTOTAL, Staff/Personnel				

Total Project

Total Project Cost	Funding Requested for this subcontract	Funding from other sources*	Comments, explanation

*Sources may include in-kind or financial donations from your organization, other organization. This information is not required, but will help us to understand your overall resources to implement the proposed project.

**Hourly rates should be fully loaded to include fringe benefits, overhead, and administrative fee.

NHLBI's *Learn More Breathe Better®*
2025-2026 Community Subcontract Program
Appendix B: Human Subjects Protection Review Executive Summary

The following should be provided as an appendix accompanying your proposal. Failure to complete may result in a disqualification of the proposal submission. This appendix should be no more than 4 pages in length and does not count against the 10-page limit specified for the core response to the Request for Proposals (RFP).

For more information about human subjects protection requirements and whether your research may need Institutional Review Board oversight, please see Section 6 of the RFP.

1. In 100 words or less, please provide a brief overview of the study protocol, including justification for conducting this research. [See the ***Understanding the Challenge and Current COPD Landscape*** section of your grant application for language to use here.]

2. In 200 words or less, please describe the research activities you will be conducting (e.g., description of subjects; discussion of the types of information being collected, including any "sensitive" data that will be gathered). [See the ***Strategies and Methods*** section of your grant application for language to use here.]

3. In 100 words or less, please list inclusion/exclusion criteria for human subjects (e.g., people ages 45 and older living in rural communities).

4. In 100 words or less, please describe the informed consent process, including, but not limited to, how and when informed consent/assent will be collected and who will be obtaining it.

5. If you are requesting a waiver or modification of informed consent (e.g., you are collecting data virtually such as online or via telephone), please provide appropriate justification for this request, in 200 words or less.

    a. Describe potential risks in conducting this study, including plans to minimize those risks (100 words or less). Include physical, psychological, or emotional harm or discomfort.

    b. Explain how the risks are reasonable in relation to the benefits (100 words or less).

6. Describe direct benefits to be gained by the subjects, in 200 words or less. **Note: Except for medical research studies, most research doesn't involve a direct benefit to subjects. If this is true for your project, please use the following language: "There is no direct benefit to participants."**

7. In 200 words or less, please describe indirect benefits such as knowledge gained for society. If no benefits will be gained, then include that information in this section. [See the ***Understanding the Challenge and Current COPD Landscape*** section of your proposal for possible language to use.]

8. Please provide a list of documents that will result from this study.

9. In 200 words or less, please describe confidentiality and data security and destruction procedures. This description should include a list of all data files that will be generated from any of the data collection conducted (e.g., focus group transcripts, aggregate survey responses, audio or video recordings from interviews, interview notes and observations). Please describe where these data files will be stored and how they will be protected (e.g., network security settings, restrictions on staff access, password protection, and backup systems). Please provide the date or timeframe at which all data files will be destroyed.

PART I – TERMS AND CONDITIONS

14.0 Data Rights

The NHLBI shall have unlimited rights to and ownership of all deliverables provided under this task order, including reports, recommendations, briefings, work plans and all other deliverables. This includes the deliverables provided under the basic order and any optional task deliverables exercised by the Contracting Officer. In addition, it includes any additional deliverables required by a modification. The definition of "unlimited rights" is contained in Federal Acquisition Regulation (FAR) 27.401, "Definitions." FAR clause 52.227-14, "Rights in Data-General," is hereby incorporated by reference and made a part of this contract/order.

15.0 Organizational Conflict of Interest

The offeror's attention is directed to FAR Subpart 9.5, Organizational Conflicts of Interest. Any potential conflict of interest issues will be considered prior to award of the work to be performed.

A Conflict of Interest (COI) shall be determined at the labor category level of the task order and shall be specific to the Statement of Work (SOW) as defined in the task order relative to contract sensitive or proprietary information. Because of the nature of this order, there could be a direct COI in areas related to the preparation of a SOW, the evaluation of proposal(s), and access to proprietary information. In certain circumstances where it has been determined that there is a COI, contractor staff, including subcontractors and consultants, shall sign a non-compete statement in addition to signing a non-disclosure statement. When this condition occurs, and a mitigation plan cannot adequately remove the COI to the satisfaction of the Government, then the contractor shall be precluded from proposing on future requirements related to where a particular COI exists.

PART III – FEDERAL ACQUISITION REGULATION (FAR) CLAUSES

NOTE: Notwithstanding The Terms And Conditions Listed Below, All GSA FSS Contract Terms and Conditions are in Full Effect Under This BPA.

1.0 Incorporated by Reference

The Federal Acquisition Regulation clauses and provisions and the General Services Administration Acquisition Regulation clauses and provisions, as detailed in the Contractor's Federal Supply Schedule contracts, are incorporated by reference into the task order. The clauses and provisions, in full text, are located at: http://www.gsaelibrary.gsa.gov/.

FAR CLAUSE DESCRIPTION

52.212-4 Contract Terms and Conditions—Commercial Products and Commercial Services (DEC. 2022)

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

PART IV – DEPARTMENT OF HEALTH AND HUMAN SERVICES ACQUISITION REGULATION (HHSAR) (48 CHAPTER 3) CLAUSES

1.0 Key Personnel, HHSAR 352.237-75 (December 2015)

a. The key personnel, specified in this order, are considered to be essential to work performance. At least 30 days prior to the Contractor voluntarily diverting any of the specified individuals to other programs or orders, the Contractor shall notify the Contracting Officer and shall submit a justification for the diversion or replacement and a request to replace the individual. The request must identify the proposed replacement and provide an explanation of how the replacement's skills, experience, and credentials meet or exceed the requirements of the order (including, when applicable, Human Subjects Testing requirements). If the employee of the Contractor is terminated for cause or separates from the Contractor voluntarily with less than thirty days' notice, the Contractor shall provide the maximum notice practicable under the circumstances. The Contractor shall not divert, replace, or announce any such change to key personnel without the written consent of the Contracting Officer. The order will be modified to add or delete key personnel as necessary to reflect the agreement of the parties.

(End of Clause)

b. The following individuals are considered to be essential to the work being performed hereunder:

c. In the event that any of the key personnel named in the task order are unable to perform because of death, illness, resignation from the Contractor employment, dissolution of agreement, or other reasons, the Contractor shall submit to the Contracting Officer within five (5) business days a detailed written explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any other information that the Contracting Officer deems pertinent to approve the substitution. No substitution is to be made without the prior written approval of the Contracting Officer. No increases in task order pricing will be allowed when substitutions are authorized by the Government.

d. The Contracting Officer will have the right to effect removals of any Contractor employees working under any task order at any time during the life of the task order, if those employees are deemed not to possess the proper level of competence or abilities, or otherwise found to be unsuitable for work required. In such cases, the Contractor must promptly submit the names and any other information pertinent to approvals of substitutions if requested.

e. Personnel possessing unique technical specialties may be required for certain services related to the task orders. Such personnel shall have qualifications as required by the applicable task order, and approval by the Contracting Officer must be granted, which are appropriate to the nature of the services that will be provided.

f. Failure or delays by the Contractor in providing qualified personnel, who meet the stated requirements of the task order, may be deemed sufficient reason by the Contracting Officer to recommend termination for cause.

2.0 Electronic and Information Technology Accessibility, HHSAR 352.239-74.

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

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

c. The Section 508 accessibility standards applicable to this contract and subsequently issued orders are:
300 – Functional Performance Requirements
400 – Hardware Standards General
500 – Software Standards General
600 – Support Services & Documentation Standards
WCAG Level A Requirements
WCAG Level AA Requirements

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

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

(End of clause)

3.0 Non-Discrimination in Service Delivery, HHSAR 352.237-74 (DEC 2015)

It is the policy of the Department of Health and Human Services that no person otherwise eligible will be excluded from participation in, denied the benefits of, or subjected to discrimination in the administration of HHS programs and services based on non-merit factors such as race, color, national origin, religion, sex, gender identity, sexual orientation, or disability (physical or mental). By acceptance of this contract, the contractor agrees to comply with this policy in supporting the program and in performing the services called for under this contract. The contractor shall include this clause in all sub-contracts awarded under this contract for supporting or performing the specified program and services. Accordingly, the contractor shall ensure that each of its employees, and any sub-contractor staff, is made aware of, understands, and complies with this policy.

(End of clause)

4.0 HHS Security and Privacy Language for Information and IT Procurements

4.1 Information Security and/or Physical Access Security

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 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**- All government information and information systems must be protected in accordance with

HHS/NIH policies and level of risk. At a minimum, the Contractor (and/or any subcontractor) must:

a. Protect the

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

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

Confidentiality:	[X]	Low	[ ]	Moderate	[ ]	High
Integrity:	[ ]	Low	[X]	Moderate	[ ]	High
Availability:	[X]	Low	[ ]	Moderate	[ ]	High
Overall Risk Level:	[X]	Low	[ ]	Moderate	[ ]	High

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

d. Report any discovered or unanticipated threats or hazards by either the agency or contractor, or if existing safeguards have ceased to function immediately after discovery, **within one (1) hour or less**, to the government representative(s).

e. Adopt and implement all applicable policies, procedures, controls, and standards required by the HHS/NIH 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 all applicable security and privacy policies by contacting the CO/COR or HHS/NIH security and/or privacy officials.

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

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

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

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

        [ ] No PII **[X] PII**

    c. The Contractor must support the agency with conducting a Privacy Threshold Analysis (PTA) for the information system and/ or information handled under this contract to determine whether or not a full Privacy Impact Assessment (PIA) needs to be completed.
        - If the results of the PTA show that a full PIA is needed, the Contractor must support the agency with completing a PIA for the system or information within **60 days** after completion of the PTA and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002*.
        - The Contractor must support the agency in reviewing the PIA at least every **three years** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the agency that a review is required based on a major change to the system, or when new types of PII are collected that introduces new or increased privacy risks, whichever comes first.

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

    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 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. Information and/or data must be disposed of in accordance with NIST SP 800-88, *Guidelines for Media Sanitization* .

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) must protect all government information that is or may be sensitive by securing it with a solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.

7. **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 must be used only for the purpose of carrying out the provisions of this contract and must not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its employees and subcontractors must be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any HHS records may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

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

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

8. **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol must comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.
9. **Information and Communications Technology (ICT).** ICT products and services from prohibited entities/sources must not be used/acquired in compliance with Public Law 115-232, Section 889 Parts A and B, FAR 4.21, FAR 52.204.23, FAR 52.204.24, and FAR 52.204.25. The contractor (and/or any subcontractor) must notify the government if they identify prohibited ICT products and/or services are used during the contract performance.
10. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS must enable HTTP Strict Transport Security (HSTS) to instruct compliant

browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended. Consult the *HHS Policy for Internet and Email Security* for additional information.

11. **Contract Documentation.** The Contractor must use provided templates, policies, forms and other agency documents. NIH will specify which documents/forms will be provided to comply with contract deliverables as appropriate.
12. **Standard for Encryption.** The Contractor (and/or any subcontractor) must:
    i. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.
    ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
    iii. Secure all devices (i.e.: desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and NIH-specific encryption standard requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).
    iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with current FIPS 140 validation certificate from the NIST CMVP. The Contractor must provide a written copy of the validation documentation to the COR within **15 days** of the validation.
    v. Use the Key Management system on the HHS personal identification verification (PIV) card or establish and use a key recovery mechanism to ensure the ability for authorized personnel to encrypt/decrypt information and recover encryption keys http://csrc.nist.gov/publications/ . Encryption keys must be provided to the COR upon request and at the conclusion of the contract.
13. **Contractor Non-Disclosure Agreement (NDA).** Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract must complete the OpDiv non-disclosure agreement, https://ocio.nih.gov/sites/external/files/2024-01/Nondisclosure04082020.pdf as applicable. Contractors (and/or subcontractors) must submit a copy of each signed and witnessed NDA to the Contracting Officer (CO) and/or CO Representative (COR) prior to performing any work under this acquisition.

B. TRAINING REQUIREMENTS

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/NIH Contractor Information Security Awareness, Privacy, and Records Management training course at http://irtsectraining.nih.gov/ before performing any work under this contract. Thereafter, the employees shall complete NIH 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*. Read further guidance about the NIH Role-based Training https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html.
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) must ensure that all employees performing on the contract comply with the *HHS Information Technology General Rules of Behavior, HHS Rules of Behavior for Privileged Users*.
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 NIH 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

1. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/NIH 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. In accordance with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information (PII)* , an incident is "an occurrence that

(1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies" and a privacy breach is "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose." For additional information on the HHS breach response process, please see the *HHS Policy and Plan for Preparing for and Responding to a Breach of Personally Identifiable Information (PII)*."

2. In the event of a suspected or confirmed incident or breach, the Contractor (and/or any subcontractor) must:
    i. Protect all sensitive information, including any PII created, stored, or transmitted in the performance of this contract, with encryption solution that is validated with current FIPS 140 validation certificate from the NIST CMVP.
    ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor must send NIH approved notifications to affected individuals in accordance with https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf
    iii. Report all suspected and confirmed information security and privacy incidents and breaches to the OpDiv Incident Response Team (IRT) via email at IRT@mail.nih.gov , COR, CO, OpDiv SOP (or his or her designee), and other stakeholders, including breaches involving PII, in any medium or form, including paper, oral, or electronic, as soon as possible and without unreasonable delay, no later than **one (1) hour**, and consistent with the applicable OpDiv and HHS policy and procedures, NIST standards and guidelines, as well as US-CERT notification guidelines. The types of information required in an incident report must include at a minimum: company and point of contact information, contact information, impact classifications/threat vector, and the type of information compromised. In addition, the Contractor must:
        - Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
        - Not include any sensitive information in the subject or body of any reporting e-mail; and
        - Encrypt sensitive information in attachments to email, media, etc.
    iv. Comply with OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, and HHS/NIH and NIH privacy breach response policies when handling PII breaches.

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

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:

[ ] Tier 5: Critical Sensitive and Special Sensitive National Security, including Top Secret, SCI, and "Q" access eligibility.

[ ] Tier 5SR: Reinvestigation.

[ ] Tier 4: High Risk Public Trust HRPT).

[ ] Tier 4SR: Reinvestigation.

[X] Tier 3: Non-Critical Sensitive, National Security, including Secret and "L" access eligibility.

[ ] Tier 3SR: Reinvestigation.

[ ] Tier 2S with Subject Interview: Moderate Risk Public Trust (MRPT). [ ] Tier 2SR: Reinvestigation.

[X] Tier 1: Low Risk, Non-Sensitive, including HSPD-12 Credentialing.

F. HOMELAND SECURITY PRESIDENTIAL DIRECTIVE (HSPD)-12

The Contractor (and/or any subcontractor) and its employees must comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; OMB M-05-24; OMB M-19-17; FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors; HHS HSPD-12 policy; and Executive Order 13467, Part 1 §1.2.
For additional information, see HSPD-12 policy at:
https://www.dhs.gov/homeland- security-presidential-directive-12

G. ROSTER

The Contractor (and/or any subcontractor) must submit a roster by name, position, e-mail address, phone number and responsibility, of all staff working under this acquisition where the Contractor will develop, have the ability to access, or host and/or maintain a government information system(s). The roster must be submitted to the COR and/or CO within **fourteen (14) calendar days** of the effective date of this contract. Any revisions to the roster as a result of

staffing changes must be submitted within **seven (7) calendar days** of the change. The COR will notify the Contractor of the appropriate level of investigation required for each staff member. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for Contractor use at: https://oamp.od.nih.gov/nih-document-generation-system/dgs-workform-information/attachment-files-section-jh
If the employee is filling a new position, the Contractor must provide a position description and the Government will determine the appropriate suitability level. Upon receipt of the Government's notification of applicable Suitability Investigations required, the Contractor shall complete and submit the required forms within 30 days of the notification.

H. CONTRACT INITIATION AND EXPIRATION

1. **General Security Requirements.** The Contractor (and/or any subcontractor) must comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information systems development or enhancement tasks supported by the contractor must follow the HHS EPLC framework and methodology and in accordance with the HHS Contract Closeout Directive (2018) found at: https://oamp.od.nih.gov/sites/default/files/DGS/contracting-forms/HHS-Closeout-Directive-2018.pdf . HHS EA requirements are located at: https://www.hhs.gov/web/governance/digital-strategy/it-policy-archive/hhs-policy-for-enterprise-architecture.html and NIH EA requirements are located at: https://ocio.nih.gov/enterprise-architecture
2. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to HHS System Development Life Cycle requirements, at a minimum, for system development and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.
3. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) must provide all required documentation in accordance with the NIH Media Sanitization and Disposal Policy 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) must notify the CO and/or COR and system ISSO within fifteen days before an employee stops working under this contract.
5. **Contractor Responsibilities upon Physical Completion of the Contract.** The Contractor (and/or any subcontractors) must return all government information and IT resources (i.e., government information in non- government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR. Additionally, the Contractor must provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems, including backup systems and media used during contract performance, in accordance with HHS and/or NIH policies.
6. The Contractor (and/or any subcontractor) must perform and document the actions identified in the NIH Employee Separation Checklist https://ocio.nih.gov/sites/external/files/2024-01/Emp-sep-checklist.pdf when an

employee terminates work under this contract within 2 days of the employee's exit from the contract. All documentation must be available to the CO and/or COR upon request.

I. RECORDS MANAGEMENT AND RETENTION

1. The Contractor (and/or any subcontractor) must maintain all information in accordance with Executive Order 13556 -- Controlled Unclassified Information, National Archives and Records Administration (NARA) records retention policies and schedules and *HHS Policy for Records Management* and NIH policies and must not dispose of any records unless authorized by HHS/NIH.
2. In the event that a contractor (and/or any subcontractor) accidentally disposes of or destroys a record without proper authorization, he/she must document and report the incident in accordance with HHS/ NIH policies.

J. HIGH VALUE ASSET (HVA)

If a system is identified as HVA,[23] the Contractor must comply with the HHS Policy for the High Value Asset (HVA) Program and the DHS HVA Control Overlay[24] in addition to the above requirements.

ARTICLE H.57.3. GOVERNMENT INFORMATION PROCESSED ON GOCO OR COCO SYSTEMS

1. SECURITY REQUIREMENTS FOR GOVERNMENT-OWNED/CONTRACTOR-OPERATED (GOCO)AND CONTRACTOR-OWNED/CONTRACTOR-OPERATED (COCO) RESOURCES

a. **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), 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.

b. **Assessment and Authorization (A&A)-** A valid authority to operate (ATO) certifies that the Contractor's information system meets the contract's requirements to protect the agency data. If the system under this contract does not have a valid ATO, the Contractor (and/or any subcontractor) shall work with the agency and supply the deliverables required to complete the ATO within the specified timeline(s) within three (3) months after contract award. The Contractor shall conduct the A&A requirements in accordance with HHS 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, Contracting Officer Representative 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.
NIH acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the system security and privacy controls are implemented and operating effectively.

i. **A&A Package Deliverables -** The Contractor (and/or any subcontractor) shall provide an A&A package within 30 days of contract award to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package. The NIH Assessment and Authorization Process is found at: https://wiki.nci.nih.gov/download/attachments/404161271/NCI%20AA%20Process%20-3P-CM-CoLo%20v1.4.pdf?version=1&modificationDate=1624383553000&api=v2

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 NIH 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 30 days after the contract award. The security assessment shall be conducted by the assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS and NIH policies. The assessor will document the assessment results in the SAR.*The NIH should determine which security control baseline applies and then make a determination on the appropriateness/necessity of obtaining an independent assessment. Assessments of controls can be performed by Contractor, government, or third parties, with third party verification considered the strongest. If independent assessment is required, include statement below.*
Thereafter, the Contractor, in coordination with the NIH shall conduct/assist in the assessment of the security controls and update the SAR at least annually.

Independent Assessment - due 90 days after the 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 30 days after contract award. The POA&M shall be documented consistent with the HHS Standard for Plan of Action and Milestones and NIH policies. All findings/weaknesses shall be documented in the POA&M and remediated/mitigated from the date the weaknesses are formally identified and documented by the timelines below:

Critical within 30 days:
High within 60 days;
Medium within 1 year;
and Low within 1 year.

The NIH 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, NIH 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 60 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 NIH 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.

ii. **Information Security Continuous Monitoring** - Upon the government issuance of an Authority to Operate (ATO), the Contractor (and/or subcontractor)-owned/operated systems that input, store, process, output, and/ or transmit government information, 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:

iii. **Annual Assessment/ Penetration (Pen) Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) every two (2) years on high-risk systems, 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 A& A documentation (SSP, POA& M, Contingency Plan, etc.) and provide updates by specified due date provided by the Contracting Officer Representative.

iv. **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 60 days after contract award. 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.

v. **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 within 60 days. The Contractor shall maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP- compliant automated tools.

vi. **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 within 30 days of the contract award.

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

viii. **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.

ix. **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).

c. **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:

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

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

    ii. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of

the Contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

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

d. **End of Life Compliance-** The Contractor (and/or any subcontractor) must use Commercial off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the HHS waiver process (approved by HHS CISO). 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.

e. **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:

i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS and FIPS 140-3 encryption standards.
ii. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB), and HHS Minimum Security Configuration Standards;
iii. Maintain the latest operating system patch release and anti-virus software definitions within 15 days.
iv. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching and ensure changes in hardware and software do not alter the approved configuration settings; and
v. Automate configuration settings and configuration management in accordance with HHS 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.

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

g. **Information and Communications Technology (ICT) Cybersecurity Supply Chain Risk Management (C-SCRM) requirements.** The Contractor (and/or any subcontractor) must

secure their ICT supply chain in compliance with *HHS Policy for Cyber Supply Chain Risk Management* and Public Law 115-232 § 889. At a minimum, they must implement the following:

i. Develop rules for suppliers' development methods, techniques, or practices;
ii. Use of secondary market components;
iii. Prohibit counterfeit products;
iv. Dispose and/or retain elements such as components, data, or intellectual property securely;
v. Ensure adequate supply of components;
vi. Require external providers handling federal information or operating systems on behalf of the federal government to meet the same security and privacy requirements as federal agencies;
vii. Require external providers to express security and privacy requirements (including the controls for systems processing, storing, or transmitting federal information) in contracts or other formal agreements;
viii. Establish Service Level Agreements (SLAs), patching vehicles and disclosure requirements in the case of a security incident or new vulnerability being discovered; and
ix. Ensure that the supplier applies same contractual requirements to any sub-contractors/suppliers that they involve in the provision of the product or service to the customer; and
x. Prohibit the use of covered telecommunications and video surveillance equipment or services.

ARTICLE H.57.4. CLOUD SERVICES

1. **HHS FedRAMP (Federal Risk and Authorization Management Program) Privacy and Security Requirements**

The Contractor (and/or any subcontractor) shall be responsible for the following privacy and security requirements:

a. **FedRAMP Compliant ATO**. Comply with requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor must submit a plan to obtain a FedRAMP compliant ATO by 30 days of the contract award.
    i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov).
    ii. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.
b. **Data Jurisdiction** - The Contractor must store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS) if so required as stated in section C.
c. **Service Level Agreements** - Add when applicable/ Mark as Not Applicable _____ The Contractor must understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with NIH to develop and maintain an SLA.
d. **Interconnection Agreements/ Memorandum of Agreements** - Add when applicable/ Mark as Not Applicable ____ The Contractor must establish and maintain Interconnection

Agreements and or Memorandum of Agreements/ Understanding in accordance with HHS/ NIH policies.

2. **Protection of Information in a Cloud Environment**

a. If Contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/ or company trade secrets and in accordance with HHS/ NIH policies.

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

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

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

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

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

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

3. **Assessment and Authorization (A&A) Process**

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

    i. In addition to the FedRAMP compliant ATO, the contractor shall complete and maintain an agency A& A package to obtain agency ATO prior to system deployment/ service implementation. The agency ATO must be approved by the NIH authorizing official (AO) prior to implementation of system and/ or service being acquired.
    ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third- party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited

3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non- accredited, independent assessor.

iii. For all acquired cloud services, the A& A package must contain the following documentation: SSP, SAR, POA& M, Authorization Letter, CP and CPT report, E- Authorization (if applicable), PTA/ PIA (if applicable), Interconnection/ Data Use Agreements (if applicable), Authorization Letter, Configuration Management Plan (if applicable), Configuration Baseline, Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/ NIH policies.

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

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

d. The Contractor (and/or any subcontractor) must mitigate security risks for which they are responsible, including those identified during A& A and continuous monitoring activities. All vulnerabilities and other risk findings must be remediated by the prescribed timelines from discovery: (1) critical vulnerabilities no later than thirty (30) days and (2) high, medium and low vulnerabilities no later than sixty (60) days. In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they must be added to the designated POA& M and mitigated within the newly designated timelines 30 days. HHS will determine the risk rating of vulnerabilities using FedRAMP baselines.

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

4. **Reporting and Continuous Monitoring**

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

b. At a minimum, the Contractor must provide the following artifacts/deliverables on a monthly basis as directed by the Contracting Officer/Contracting Officer Representative:

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

c. **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:

i. **Annual Assessment/Pen Test** - Assess the system security and privacy controls (or ensure an assessment of the controls is conducted) at least annually to determine the implemented security and privacy controls are operating as intended and producing the desired results (this may involve penetration testing conducted by the agency or independent third-party. In addition, review all relevant A&A documentation (SSP, POA&M, Contingency Plan, etc.) and provide updates by specified due date provided by the Contracting Officer Representative.
ii. **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 60 days after contract award. IT asset inventory information must include IP address, machine name, operating system level, security patch level, and SCAP-compliant format information. The Contractor must maintain a capability to provide an inventory of 100% of its IT assets using SCAP-compliant automated tools.
iii. **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 within 60 days. The

Contractor must maintain a capability to provide security configuration compliance information for 100% of its IT assets using SCAP-compliant automated tools.

iv. **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 must actively manage system vulnerabilities using automated tools and technologies where practicable and in accordance with HHS policy. Automated tools must 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 within 30 days of the contract award.

v. **Patching and Vulnerability Remediation** - Install vendor released security patches and remediate critical and high vulnerabilities in systems processing government information in an expedited manner, within vendor and agency specified timeframes.

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

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

viii. A security control assessment must be conducted by a FedRAMP third-party assessment organization (3PAO) for the initial ATO and annually thereafter or whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

5. **Configuration Baseline**

a. The Contractor must certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), DISA Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS- identified configuration baseline. The standard installation, operation, maintenance, updates, and/ or patching of software must not alter the configuration settings from the approved HHS/NIH.

b. The Contractor must configure its computers that contain HHS data with the latest applicable United States Government Configuration Baseline (USGCB) and/ or other approved HHS IT Security Configurations. (See: https://usgcb.nist.gov/). Note: Approved security configurations include, but are not limited to, those published by the Department, the NIH, and the National Institute of Standards and Technology (NIST). NIH may have security configurations that are more stringent than the minimum baseline set by the Department or NIST. When incorporating such security configuration requirements in solicitations and contracts, the NIH CISO and/ or Information System Security Officer (ISSO) must be consulted to determine the appropriate configuration reference for a particular system or services acquisition.)

c. The Contractor must apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS and must adhere to all NIH configuration standards and policies (See: https://ocio.nih.gov/it-governance/it-policy-standards-and-guidance.

d. The Contractor must ensure IT applications operated on behalf of HHS are fully functional and operate correctly on systems configured in accordance with the above configuration requirements. The Contractor must use Security Content Automation Protocol (SCAP)-validated tools with USGCB Scanner capability to ensure its products operate correctly with USGCB configurations and do not alter USCGB settings - (See: https://csrc.nist.gov/projects/scap-validation-program). The Contractor must test applicable product versions with all relevant and current updates and patches installed. The Contractor must ensure currently supported versions of information technology products met the latest USGCB major version and subsequent major versions.

e. The Contractor must ensure IT applications designed for end users run in the standard user context without requiring elevated administrative privileges.

f. The Contractor must ensure hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above.

g. The Contractor must (1) include Federal Information Processing Standard (FIPS) 201-compliant (See: https://csrc.nist.gov/csrc/media/publications/fips/201/1/archive/2006-06-26/documents/fips-201-1-chng1.pdf), Homeland Security Presidential Directive 12 (HSPD-12) card readers with the purchase of servers, desktops, and laptops; and (2) comply with FAR Subpart 4.13, Personal Identity Verification.

h. The Contractor must ensure that its subcontractors (at all tiers) which perform work under this contract comply with the requirements contained in this clause.

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

6. **Incident Reporting**

a. The Contractor (and/or any subcontractor) must respond to all alerts/Indicators of Compromise (IOCs) provided by HHS Computer Security Incident Response Center (CSIRC)/NIH IRT teams within one (1) hour of the discovery of the loss/theft, 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 cyber security 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) must:

    i. 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 140-3 validated encryption.

ii. NOT notify affected individuals unless so instructed by the Contracting Officer or designated representative. If so instructed by the Contracting Officer or representative, the Contractor shall send NIH approved notifications to affected individuals in accordance with https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf

iii. Report all suspected and confirmed information security and privacy incidents and breaches to the NIH Incident Response Team (IRT) IRT@nih.gov, COR, CO, the NIH Office of the 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 of the discovery of the loss/theft, and consistent with the applicable NIH 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 must:

- Cooperate and exchange any information, as determined by the Agency, necessary to effectively manage or mitigate a suspected or confirmed breach;
- Not include any sensitive information in the subject or body of any reporting e-mail; and
- Encrypt sensitive information in attachments to email, media, etc.

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

c. 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.

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

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

i. Conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/NIH personnel, or agents acting on behalf of HHS/NIH, using agency-operated equipment and/or specified tools. The Contractor may choose to

run its own automated scans or audits, provided the scanning tools and configuration settings are compliant with NIST Security Content Automation Protocol (SCAP) standards and have been approved by the agency. The agency may request the Contractor's scanning results and, at the agency discretion, accept those in lieu of agency performed vulnerability scans.

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

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

7. **Media Transport**

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

b. All information, devices and media must be encrypted with HHS-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

8. **Boundary Protection: Trusted Internet Connections (TIC)**

a. The Contractor shall ensure that government information, other than unrestricted information, being transmitted from federal government entities to external entities using cloud services is inspected by Trusted Internet Connection (TIC) processes.

b. The Contractor shall route all external connections through a TIC.

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

ARTICLE H.57.5.2. NON-COMMERCIAL AND OPEN SOURCE COMPUTER SOFTWARE PROCUREMENTS

The Contractor (and/or any subcontractor) must follow secure coding best practice requirements, as directed by the 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. The Contractor will be liable for malicious or defective code or failure to reduce risk.

ARTICLE H.57.5.3. INFORMATION TECHNOLOGY APPLICATION DESIGN, DEVELOPMENT, OR SUPPORT

a. The Contractor (and/or any subcontractor) must ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.
b. The Contractor (and/or any subcontractor) must 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.
c. The Contractor (and/or any subcontractor) must ensure that computer software developed on behalf of HHS or tailored from an open-source product, is fully functional and operates correctly on systems configured in accordance with government policy and federal configuration standards. The contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS environment. No sensitive data must be used during software testing.
d. The Contractor (and/or any subcontractor) must protect information that is deemed sensitive from unauthorized disclosure to persons, organizations or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

ARTICLE H.1.4. PHYSICAL ACCESS TO GOVERNMENT CONTROLLED FACILITIES

Refer to the GSA Schedule SECTION H Clause - Government Information and Physical Access Security.

ARTICLE H.2. ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY, HHSAR 352.239-74 (DECEMBER 2015)

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

b. The Section 508 accessibility standards applicable to this contract and subsequently issued Task Orders are identified below. The Contractor must provide any necessary updates to the submitted HHS Product Assessment Template(s) at the end of each contract or order exceeding the simplified acquisition threshold (see FAR 2.101) when the contract or order duration is one year or less. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of

the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

c. The Section 508 accessibility standards applicable to this Task Order are:

- Electronic Reports/Deliverables are submitted in electronic format which shall be compliant with Section 508 of the Rehabilitation Act of 1973.
- 300 Functional Performance Requirements
    a. Technical Standards: 1194.31 Functional performance criteria
- 600 Support Services & Documentation Standards comparable with
    a. Technical Standards: 1194.41 Information, documentation and support
- WCAG Level A Requirements (overlaps with Chapter 4 and 5)
- WCAG Level AA Requirements (overlaps with Chapter 4 and 5)
- In the event of a modification(s) to this contract or order, which adds new EIT supplies or services or revises the type of, or specifications for, supplies or services, the Contracting Officer may require that the Contractor submit a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found under Section 508 policy on the HHS website: (http://www.hhs.gov/web/508). If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the contract, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.
- If this is an Indefinite Delivery contract, a Blanket Purchase Agreement or a Basic Ordering Agreement, the task/delivery order requests that include EIT supplies or services will define the specifications and accessibility standards for the order. In those cases, the Contractor may be required to provide a completed HHS Section 508 Product Assessment Template and any other additional information necessary to assist the Government in determining that the EIT supplies or services conform to Section 508 accessibility standards. Instructions for documenting accessibility via the HHS Section 508 Product Assessment Template may be found at http://www.hhs.gov/web/508. If it is determined by the Government that EIT supplies and services provided by the Contractor do not conform to the described accessibility standards in the provided documentation, remediation of the supplies or services to the level of conformance specified in the contract will be the responsibility of the Contractor at its own expense.

(End of clause)

PART V – NATIONAL INSTITUTES OF HEALTH (NIH) CLAUSES

1.0 Access to National Institutes of Health (NIH) Electronic Mail

All Contractor staff that have access to and use of NIH electronic mail (e-mail) must identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, the Contractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each Contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent.

2.0 Confidentiality of Information

a. Confidential information, as used in this section, 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.

b. The Contracting Officer and the Contractor may, by mutual consent, identify elsewhere in this task order specific information and/or categories of information which the Government will furnish to the Contractor or that the Contractor is expected to generate which is confidential. Similarly, the Contracting Officer and the Contractor may, by mutual consent, identify such confidential information from time to time during the performance of the task order. Failure to agree will be settled pursuant to the "Disputes" clause.

c. If it is established elsewhere in this task order that information to be utilized under this task order, or a portion thereof, is subject to the Privacy Act, the Contractor will follow the rules and procedures of disclosure set forth in the Privacy Act of 1974, 5 U.S.C. 552a, and implementing regulations and policies, with respect to systems of records determined to be subject to the Privacy Act.

d. Confidential information, as defined in paragraph (a) of this section, shall not be disclosed without the prior written consent of the individual, institution, or organization.

e. Whenever the Contractor is uncertain with regard to the proper handling of material under the task order, or if the material in question is subject to the Privacy Act or is confidential information subject to the provisions of this section, the Contractor should obtain a written determination from the Contracting Officer prior to any release, disclosure, dissemination, or publication.

f. Contracting Officer's determination will reflect the result of internal coordination with appropriate program and legal officials.

g. The provisions of paragraph (d) of this section shall not apply to conflicting or overlapping provisions in other Federal, State, or local laws.

3.0 Use of Funds for Conferences, Meetings, and Food

a. The Contractor shall not use contract funds to conduct meetings or conferences without prior written Contracting Officer approval.

b. In addition, the use of contract funds to purchase food for meals, light refreshments, or beverages is expressly prohibited.

4.0 Use of Funds for Promotional Items

The Contractor shall not use contract funds to purchase promotional items. Promotional items include, but are not limited to: clothing and commemorative items, such as pens, mugs/cups, folders/folios, lanyards, and conference bags that are sometimes provided to visitors, employees, grantees, or conference attendees. This includes items or tokens given to individuals, as these are considered personal gifts for which contract funds may not be expended.