NHLBI's *The Heart Truth®*

2021-2022 Community Subcontract Program

Appendix A: Budget Template for NHLBI's *The Heart Truth* Community Subcontract 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 *The Heart Truth®*
2021-2022 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 or visit https://www.hhs.gov/ohrp/.

1. In 100 words or less, please provide a brief overview of the protocol for your proposed project, including justification for conducting this research. [See the ***Understanding the Challenge and Current Heart Disease 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 any criteria you will use in recruiting human subjects (e.g. age, gender, health status).

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. For more information on informed consent visit this website.

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).

    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. [See the ***Understanding the Challenge and Current Heart Disease 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.

NHLBI's *The Heart Truth®*
2021-2022 Community Subcontract Program
Appendix C: Applicable "Government Contract" Requirements

The Parties acknowledge and agree that, under this Agreement, Awardee will be providing services that qualify as "commercial items" within the meaning of Federal Acquisition Regulation ("FAR") 2.101. Therefore, consistent with FAR 52.212-5(a), the Parties agree that the only FAR provision clauses from the Contract incorporated into this Agreement are

a) FAR 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note));

b) FAR 52-203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5);

c) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jul 2013) (Pub. L. 109-282);

d) FAR 52.219-8 Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1,500,000 for construction of any public facility), the awardee must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities;

e) FAR 52.222-26 Equal Employment Opportunity (Mar 2007) (E.O. 11246);

f) FAR 52.222-35 Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (July 2014) (38 U.S. C. 4212(a));

g) FAR 52.222-36 Affirmative Action for Workers with Disabilities (July 2014) (20 U.S.C. 793);

h) FAR 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496);

i) FAR 52.222-54 – Employment Eligibility Verification (Aug 2013) Employment Eligibility Verification: Pursuant to clause 52.222-54 of the Federal Acquisition Regulation ("FAR"), Awardee shall enroll in e- Verify as a federal contractor within 30 calendar days of the Effective Date of this Amendment if they are not presently enrolled at the time of execution. Within 90 days of enrollment in the E-Verify program, Awardee must begin to use E-Verify to verify employment eligibility of all hires within 3 business days of the hiring; and for each employee assigned to this Agreement, Awardee shall initiate verification within 90 calendar days after Awardee's date of enrollment or within 30 calendar days of the employee's assignment to this Agreement, whichever date is later. Awardee shall comply with the requirements of the E- Verify program

MOU throughout the Term of this Subcontract. Awardee shall include the requirements of this clause in any second- tier subcontracts for services performed in the U.S. with a value greater than $3,000.00. Subcontractor should refer to FAR Clause 52.222-54 for additional details regarding this requirement. Said clause can be found in its entirety at https://www.acquisition.gov/far/index.html. FAR clause 52.222-54 is incorporated herein by reference with the same force and effect as if said clause was given in full text.

j) FAR 52.247-64 Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

The term "Contractor" and similar terms in these FAR provisions shall be construed to mean Awardee for the purposes of their application to this Agreement.

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

2.0 Information and Physical Access Security

The Homeland Security Presidential Directive (HSPD)-12 and the Federal Information Security Management Act of 2002 (P.L. 107-347) (FISMA) requires each agency to develop, document, and implement an agency-wide information security program to safeguard information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor (including subcontractor), or other source.

3.0 HHS-Controlled Facilities and Information Systems Security

a. To perform the work specified herein, Contractor personnel are expected to have routine (1) physical access to an HHS-controlled facility; (2) physical access to an HHS- controlled information system; (3) access to sensitive HHS data or information, whether in an HHS-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3).

b. To gain routine physical access to an HHS-controlled information system, and/or access to sensitive data or information, the Contractor and its employees shall comply with Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors; Office of Management and Budget Memorandum (M-05-24); and Federal Information Processing Standards Publication (FIPS PUB) Number 201; and with the personal identity verification and investigations procedures contained in the following documents:

1. HHS-OCIO Information Systems Security and Privacy Policy https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/index.html

2. HHS HSPD-12 Policy Document, v. 2.0
https://www.dhs.gov/homeland-security-presidential-directive-12

3. Information regarding background checks/badges
https://ors.od.nih.gov/ser/dpsac/Pages/Home.aspx

(a) Position Sensitivity Levels:
This contract (Task Order) will entail the following position sensitivity levels:

(i) [ ] Level 6: Public Trust - High Risk. Contractor / subcontractor employees assigned to Level 6 positions shall undergo a Suitability Determination and Background Investigation (MBI).

(ii) [ ] Level 5: Public Trust - Moderate Risk. Contractor / subcontractor employees assigned to Level 5 positions with no previous investigation and approval shall undergo a Suitability Determination and a Minimum Background Investigation (MBI), or a Limited Background Investigation (LBI).

(iii) [**X**] Level 1: Non-Sensitive. Contractor/subcontractor employees assigned to Level 1 positions shall undergo a Suitability Determination and a National Agency Check and Inquiry Investigation (NACI).

(iv) The personnel investigation procedures for Contractor personnel require that (upon award) the Contractor prepare and submit background check/investigation forms based on the type of investigation required. The minimum Government investigation for a non-sensitive position is a National Agency Check and Inquiries (NACI) with fingerprinting. More restricted positions - i.e., those above non-sensitive, require more extensive documentation and investigation.

(v) As part of its proposal, and if the anticipated position sensitivity levels are specified in paragraph (d) above, the Offeror shall notify the Contracting Officer of (1) its proposed personnel who will be subject to a background check/investigation and (2) whether any of its proposed personnel who will work under the contract have previously been the subject of national agency checks or background investigations.

(vi) Upon award, the Contractor shall submit a roster, by name, position, e-mail address, phone number and responsibility, of all staff (including subcontractor staff) working under the contract that will develop, have the ability to access

and/or maintain a Federal Information System(s). The roster shall be submitted to the Contracting Officer's Representative (COR), with a copy to the Contracting Officer, within 14 calendar days after the effective date of the contract. The Contracting Officer shall notify the Contractor of the appropriate level of suitability investigations to be performed. An electronic template, "Roster of Employees Requiring Suitability Investigations," is available for contractor use at: https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/SuitabilityRoster_10-15-12.xlsx.

(vii) 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.

(viii) The Contractor shall notify the Contracting Officer in advance when any new personnel, who are subject to a background check/investigation, will work under the contract and if they have previously been the subject of national agency checks or background investigations.

(ix) All contractor and subcontractor employees shall comply with the conditions established for their designated position sensitivity level prior to performing any work under this contract.

(x) Contractors may begin work after the fingerprint check has been completed.

(b) Investigations are expensive and may delay performance, regardless of the outcome of the investigation. Delays associated with rejections and consequent re-investigations may not be excusable in accordance with the FAR clause, Excusable Delays - see FAR 52.249-14. Accordingly, the Contractor shall ensure that any additional employees whose names it submits for work under this contract have a reasonable chance for approval.

(c) Typically, the Government investigates personnel at no cost to the Contractor. However, multiple investigations for the same position may, at the Contracting Officer's discretion, justify reduction(s) in the contract price of no more than the cost of the additional investigation(s). Accordingly, if position sensitivity levels are specified in paragraph (b) above, the Offeror shall ensure that the employees it proposes for work under this contract/order have a reasonable chance for approval.

(d) The Contractor shall include language similar to this "HHS Controlled Facilities and Information Systems Security" language in all subcontracts that require subcontractor personnel to have the same frequency and duration of (1) physical access to an HHS-controlled facility; (2) logical access to an HHS-controlled information system; (3) access to sensitive HHS data/information, whether in an HHS-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3).

(e) The Contractor shall direct inquiries, including requests for forms and assistance, to the Contracting Officer.

(f) Within 7 calendar days after the Government's final acceptance of the work under this contract, or upon termination of the contract, the Contractor shall return all identification badges to the Contracting Officer or designee.

4.0 Standard for Security Configurations

a. The Contractor shall configure its computers that contain HHS data with the applicable Federal Desktop Core Configuration (FDCC) (see http://nvd.nist.gov/fdcc/index.cfm) and ensure that its computers have and maintain the latest operating system patch level and anti-virus software level. ***Note:*** FDCC is applicable to all computing systems using Windows XPTM and Windows VistaTM, including desktops and laptops - regardless of function - but not including servers.

b. The Contractor shall apply approved security configurations to information technology (IT) that is used to process information on behalf of HHS. The following security configuration requirements apply:

1. The Contractor shall 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 shall use Security Content Automation Protocol (SCAP)-validated tools with FDCC Scanner capability to ensure its products operate correctly with FDCC configurations and do not alter FDCC settings - see http://scap.nist.gov/validation. The Contractor shall test applicable product versions with all relevant and current updates and patches installed. The Contractor shall ensure currently supported versions of information technology products met the latest FDCC major version and subsequent major versions.

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

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

4. The Contractor shall (1) include Federal Information Processing Standard (FIPS) 201-compliant (https://csrc.nist.gov/publications/detail/fips/201/2/final), 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.

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

5.0 Standard for Encryption Language

a. The Contractor shall use Federal Information processing Standard (FIPS) 140-2-compliant encryption (Security) Requirements for Cryptographic Module, as amended) to protect all instances of HHS sensitive information during storage and transmission. (Note: The Government has determined that HHS information under this contract is considered "sensitive" in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, dated February 2004).

b. The Contractor shall verify that the selected encryption product has been validated under the Cryptographic Module Validation Program (see https://csrc.nist.gov/projects/cryptographic-module-validation-program) to confirm compliance with FIPS 140-2 (as amended). The Contractor shall provide a written copy of the validation documentation to the Contracting Officer and the Contracting Officer's Representative.

c. The Contractor shall use the Key Management Key (see FIPS 201, Chapter 4, as amended) on the HHS personal identification verification (PIV) card; or alternatively, the Contractor shall establish and use a key recovery mechanism to ensure the ability for authorized personnel to decrypt and recover all encrypted information (see http://csrc.nist.gov/drivers/documents/ombencryption-guidance.pdf). The Contractor shall notify the Contracting Officer and the Contracting Officer's Representative of personnel authorized to decrypt and recover all encrypted information.

d. The Contractor shall securely generate and manage encryption keys to prevent unauthorized decryption of information in accordance with FIPS 140-2 (as amended).

e. The Contractor shall ensure that this standard is incorporated into the Contractor's property management/control system or establish a separate procedure to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive HHS information.

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

6.0 Security Requirements for Federal Information Technology Resources

a. **Applicability.** This clause applies whether the entire contract or order (hereafter "contract"), or portion thereof, includes information technology resources or services in which the Contractor has physical or logical (electronic) access to, or operates a Department of Health and Human Services (HHS) system containing, information that directly supports HHS' mission. The term "information technology (IT)", as used in this clause, 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. This clause does not apply to national security systems as defined in FISMA.

b. **Contractor responsibilities.** The Contractor is responsible for the following:

1. Protecting Federal information and Federal information systems in order to ensure their –

   (a) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non- repudiation and authenticity;

   (b) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

   (c) Availability, which means ensuring timely and reliable access to and use of information.

2. Providing security of any Contractor systems, and information contained therein, connected to an HHS network or operated by the Contractor, regardless of location, on behalf of HHS.

3. Adopting, and implementing, at a minimum, the policies, procedures, controls and standards of the HHS Information Security Program to ensure the integrity, confidentiality, and availability of Federal information and Federal information systems for which the Contractor is responsible under this contract or to which it may otherwise have access under this contract. The HHS Information Security Program is outlined in the HHS Information Security Program Policy, which is available on the HHS Office of the Chief Information Officer's (OCIO) Web site.

c. **Contractor security deliverables.** In accordance with the timeframes specified, the Contractor shall prepare and submit the following security documents to the Contracting Officer for review, comment, and acceptance:

1. **FIPS 199 Standards for Security Categorization of Federal Information and Information Systems Assessment (FIPS 199 Assessment)** – due within 30 days after contract award. The FIPS 199 Assessment shall be consistent with the cited NIST standard. After resolution of any comments by the Government on the draft FIPS 199 Assessment, the Contracting Officer shall accept the FIPS 199 Assessment and incorporate the Contractor's final version into the contract.

d. **Personal identity verification.** The Contractor shall identify its employees with access to systems operated by the Contractor for HHS or connected to HHS systems and networks. The Contracting Officer's Representative (COR) shall identify, for those identified employees, position sensitivity levels that are commensurate with the responsibilities and risks associated with their assigned positions. The Contractor shall comply with the HSPD-12 requirements contained in "HHS-Controlled Facilities and Information Systems Security" requirements specified in the SOW of this contract.

e. **Contractor and subcontractor employee training.** The Contractor shall ensure that its employees, and those of its subcontractors, performing under this contract complete HHS-furnished initial and refresher security and privacy education and awareness training before being granted access to systems operated by the Contractor on behalf of HHS or access to HHS systems and networks. The Contractor shall provide documentation to the COR evidencing that Contractor employees have completed the required training.

f. **Government access for IT inspection.** The Contractor shall afford the Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of this contract to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation, and audit to safeguard against threats and hazards to the integrity, confidentiality, and availability, of HHS data or to the protection of information systems operated on behalf of HHS.

g. **Subcontracts.** The Contractor shall incorporate the substance of this clause in all subcontracts that require protection of Federal information and Federal information systems as described in paragraph (a) of this clause, including those subcontracts that –

1. Have physical or electronic access to HHS' computer systems, networks, or IT infrastructure; or

2. Use information systems to generate, store, process, or exchange data with HHS or on behalf of HHS, regardless of whether the data resides on a HHS or the Contractor's information system.

h. **Contractor employment notice.** The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment (or is no longer assigned to the HHS project under this contract), if that employee has, or had, access to HHS information systems or data.

i. **Document information.** The Contractor shall contact the Contracting Officer for any documents, information, or forms necessary to comply with the requirements of this clause.

j. **Contractor responsibilities upon physical completion of the contract.** The Contractor shall return all HHS information and IT resources provided to the Contractor during contract performance and certify that all HHS information has been purged from Contractor-owned systems used in contract performance.

k. Failure to comply. Failure on the part of the Contractor or its subcontractors to comply with the terms of this clause shall be grounds for the Contracting Officer to terminate this contract. (End of Clause)

Note: The NIST Special Publication SP-800-26, cited in subparagraph c.1. of this clause, has been superseded by NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations" for use for the assessment of security control effectiveness. See http://csrc.nist.gov/publications/PubsSPs.html to access NIST Special Publications (800 Series).

7.0 Security Categorization of Federal Information and Information Systems (FIPS 199 Assessment)

a. Information Type:

[**X**] Administrative, Management and Support Information: *See Statement of Work, Attachment 1 of this BPA.*
[**X**] Mission Based Information: *See Statement of Work, Attachment 1 of this BPA.*

Security Categories and Levels:

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

b. The Contractor shall submit a FIPS 199 Assessment within 30 days after contract award. Any differences between the Contractor's assessment and the information contained herein will be resolved, and if required, the contract will be modified to incorporate the final FIPS 199 Assessment.

8.0 Information Security Training

In addition to any training covered under paragraph (e) of HHSAR 352.239-72, the Contractor shall comply with the below training:

a. Mandatory Training

1. All Contractor employees having access to (1) Federal information or a Federal information system or (2) sensitive data/information shall complete the NIH Computer Security Awareness Training course at http://irtsectraining.nih.gov/ before performing any work under this contract. Thereafter, Contractor employees having access to the information identified above shall complete an annual NIH-specified refresher course during the life of this contract. The Contractor shall also ensure subcontractor compliance with this training requirement.

2. The Contractor shall maintain a listing by name and title of each Contractor/Subcontractor employee working on this contract and having access of the kind in paragraph a (1) above, who has completed the NIH required training. Any additional security training completed by the Contractor/Subcontractor staff shall be included on this listing. The list shall be provided to the COR and/or Contracting Officer upon request.

b. Role-based Training

1. HHS requires role-based training when responsibilities associated with a given role or position, could, upon execution, have the potential to adversely impact the security posture of one or more HHS systems. Read further guidance about "NIH Information Security Awareness and Training Policy" at: https://ocio.nih.gov/aboutus/publicinfosecurity/securitytraining/Pages/default.aspx.

2. The Contractor shall maintain a list of all information security training completed by each contractor/subcontractor employee working under this contract. The list shall be provided to the COR and/or Contracting Officer upon request.

c. Rules of Behavior

The Contractor shall ensure that all employees, including subcontractor employees, comply with the NIH Information Technology General Rules of Behavior (https://ocio.nih.gov/aboutus/publicinfosecurity/securitytraining/Pages/NIH_IT_GeneralRulesofBehavior.aspx), which are contained in the NIH Information Security Awareness Training Course http://irtsectraining.nih.gov.

9.0 Personnel Security Responsibilities

The Contractor shall comply with the below personnel security responsibilities:

a. The Contractor shall notify the Contracting Officer and the COR **within five working days** before a new employee assumes a position that requires access to HHS information systems or data, or when an employee with such access stops working on this contract. The Government will initiate a background investigation on new employees assuming a position that requires access to HHS information systems or data, and will stop pending background investigations for employees that no longer work under the contract or no longer have such access.

b. **New contractor employees who have or will have access to HHS information systems or data:** The Contractor shall provide the COR with the name, position title, e-mail address, and phone number of all new contract employees working under the contract and provide the name, position title and position sensitivity level held by the former incumbent. If an employee is filling a new position, the Contractor shall provide a position description and the Government will determine the appropriate position sensitivity level.

c. **Departing contractor employees:** The Contractor shall provide the COR with the name, position title, and position sensitivity level held by or pending for departing employees. The Contractor shall perform and document the actions identified in the Contractor Employee Separation Checklist (https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Emp-sep-checklist.pdf) when a Contractor/subcontractor employee terminates work under this contract. All documentation shall be made available to the COR upon request.

d. **Commitment to Protect Non-Public Departmental Information and Data.** The Contractor, and any subcontractors performing under this contract, shall not release, publish, or disclose non-public Departmental information to unauthorized personnel, and shall protect such information in accordance with provisions of the following laws and any other pertinent laws and regulations governing the confidentiality of such information:

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records)
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information)
- Public Law 96-511 (Paperwork Reduction Act)

Each employee, including subcontractors, having access to non-public Department information under this acquisition shall complete the "Commitment to Protect Non-Public Information - Contractor Employee Agreement" located at: https://ocio.nih.gov/aboutus/publicinfosecurity/acquisition/Documents/Nondisclosure.pdf. A copy of each signed and witnessed Non-Disclosure agreement shall be submitted to the Project Officer/COR prior to performing any work under this acquisition.

10.0 Loss and/or Disclosure of Personally Identifiable Information (PII) - Notification of Data Breach

The Contractor shall report all suspected or confirmed incidents involving the loss and/or disclosure of PII in electronic or physical form. Notification shall be made to the NIH Incident Response Team (IRT) via email (IRT@mail.nih.gov) within one hour of discovering the incident. The Contractor shall follow up with IRT by completing and submitting one of the applicable two forms below within three (3) work days of incident discovery:

a. NIH PII Spillage Report

b. NIH Lost or Stolen Assets Report

11.0 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 http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards.

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

c. The Section 508 accessibility standards applicable to this BPA and subsequently issued orders are:

§ 1194.22 Web-based Intranet and Internet Information and Applications (a-p)
§ 1194.24 Video and Multimedia Products (c, d, and e)
§ 1194.31 Functional Performance Criteria (a-f)
§ 1194.41 Information, Documentation, and Support (a-c)

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)

12.0 Privacy Act, HHSAR 352.224-70 (DEC 2015)

This BPA, and subsequently issued orders, requires the Contractor to perform one or more of the following: (a) design; (b) develop; or (c) operate a Federal agency system of records to accomplish an agency function in accordance with the Privacy Act of 1974 (Act) (5 U.S.C. 552a(m)(1)) and applicable agency regulations.

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

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

(a) Identifies the system(s) of records and the design, development, or operation work the Contractor is to perform; and

(b) Specifies the disposition to be made of such records upon completion of contract performance.

(End of clause)

45 CFR Part 5b contains additional information which includes the rules of conduct and other Privacy Act requirements and can be found at: https://www.govinfo.gov/content/pkg/CFR-2014-title45-vol1/pdf/CFR-2014-title45-vol1-part5b.pdf.

The Privacy Act System of Records applicable to this project is Number 09-25-0156. This document is also available at: https://oma.od.nih.gov/forms/Privacy Documents/PAfiles/0156.htm.

13.0 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)

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 contract 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 contract. Failure to agree will be settled pursuant to the "Disputes" clause.

c. If it is established elsewhere in this contract that information to be utilized under this contract, 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 contract, 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 Promoting Efficient Spending

a. On September 21, 2011, the Office of Management and Budget issued Memorandum M- 11-35, entitled "Eliminating Conference Spending and Promoting Efficiency in Government", emphasizing the President's priority to ensure that the Government operates with the utmost efficiency and eliminates unnecessary or wasteful spending. This was followed by the Executive Order on Delivering an Efficient, Effective, and Accountable Government (EO 13576)

and the Executive Order on Promoting Efficient Spending (EO 13589). On January 3, 2012, the Department of Health and Human Services (DHHS) issued the memorandum "HHS Policy on Promoting Efficient Spending: Use of Appropriated Funds for Conferences and Meetings, Food, Promotional Items, and Printing, and Publications" (See https://oamp.od.nih.gov/news/NIH-efficient-spending-policy).

b. In support of these directives, the NIH issued a January 30, 2012, Memorandum, entitled, "NIH Guidance Related to the HHS Policies on Promoting Efficient Spending: Use of Appropriated Funds for Conferences, Conference Grants and Meetings, Food, Promotional Items, and Printing and Publications" (See https://oamp.od.nih.gov/news/NIH-efficient-spending-policy).

c. Any contract awarded as a result of this solicitation will:

1. Specifically prohibit the use of contract funds for the provision of food for meals, light refreshments and beverages for any NIH funded meeting or conference; and

2. Limit the procurement of meeting space, promotional items, printing and publications.

4.0 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.

5.0 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.