

Request for Proposals (RFP) Fixed Price Goods or Services RFP No: USAID-AN-055

RFP Title: Request for Proposal for Participatory Implementation Research and Support on Peer Groups

Schedule:

Issuance Date of RFP: Friday, 11 February 2022
Questions Due: Friday, February 18, 2022, 17:00 (Washington, DC time)
Answers Released: Thursday, February 24, 2022, 12:00 (Washington, DC time)
Proposal Due Date: Tuesday, March 1, 2022, 17:00 (Washington, DC time) *
Tentative Award Start Date: March 14, 2022

**Offers received after this due date and time will not be accepted for consideration.*

USAID Advancing Nutrition (herein referred to as “the Project”), implemented by JSI Research & Training Institute, Inc. (JSI), is soliciting proposals to supply the above RFP title as described in the attached Terms of Reference. The Project is funded by the U.S. Agency for International Development (USAID) and is subject to all applicable Federal Acquisition Regulation (FAR) and AID Acquisition Regulations (AIDAR).

Please submit your most competitive proposal in English in accordance with the attached instructions, with all required Certifications. Any contract issued as a result of this RFP will be subject to all instructions, certifications, terms and conditions, and specifications included in this RFP. This document is a request for proposals only and in no way obligates the Project or USAID to make any award. This RFP is issued as a public notice to ensure that all interested, qualified and eligible organizations have a fair opportunity to submit proposals for funding.

All proposals, inquiries, and correspondence pertaining to this solicitation are to be directed to the attention of:

JSI Research & Training Institute, Inc.
Attn: Alexandra Green, Finance Officer
Arlington, VA, USA,
Email: procurement@advancingnutrition.org

Offers must be submitted by email with the subject “RFP No: USAID-AN-055”

JSI is committed to the highest standards of ethics and integrity in procurement. JSI has zero tolerance for fraud and strictly prohibits bribes, kickbacks, gratuities, and any other gifts in-kind or in monetary form. JSI also strictly prohibits collusion (bid rigging) between vendors and between vendors and JSI staff. JSI selects vendors on merit and will only engage vendors who demonstrate strong business ethics. Vendors must not participate in bid-rigging or attempt to offer any fee, commission, gift, gratuity, or any compensation in-kind or in monetary form to JSI employees. Vendors who do so will be disqualified from doing business with JSI. Additionally, JSI has a conflict-of-interest policy that requires staff to disclose when there is a potential conflict of interest due to the staff-member’s relationship with a vendor, and if necessary, to refrain from participation in a procurement involving that vendor. If at any time your organization has concerns that an employee has violated JSI policy, you may submit a report via JSI’s Code of Conduct Helpline at: www.jsi.ethicspoint.com.

INSTRUCTIONS TO OFFERORS

1. DEFINITIONS

Offeror: The individual or firm providing proposals for the supplies or services requested under this RFP.

Sub-Contractor/Vendor: The individual or firm awarded the services requested under the RFP in the form of a contract.

Buyer: JSI Research and Training Institute, Inc. (JSI)

2. PROPOSAL SUBMISSION AND REQUIREMENTS

No more than 1 (one) proposal may be submitted by each Offeror. Offerors are encouraged to read the RFP document in its entirety and ensure that their proposal addresses all the items cited in the proposal instructions and meets the selection criteria. All proposals must be submitted by the deadline established on the cover page of this RFP. *Offers received after this due date and time will not be accepted for consideration.*

Questions:

All questions or clarifications regarding this RFP must be in writing and submitted to procurement@advancingnutrition.org, no later than Friday, February 18, 2022, 17:00 (Washington, DC time). Questions and requests for clarification, and the responses thereto, will be posted online or circulated to all RFP recipients who have indicated interest in this RFP.

Only written answers from JSI's authorized representative will be considered official and carry weight in the RFP process and subsequent evaluation. Any answers received outside the official channel, whether received verbally or in writing, from employees or representatives of JSI, USAID Advancing Nutrition, or any other party, will not be considered official responses regarding this RFP.

Submission of Proposals:

The Offeror's proposal must be accompanied by a cover letter typed on official organizational letterhead and signed by an individual who has signatory authority for the Offeror. The Offeror must submit a complete proposal package – in electronic format – on or before the due date and time to Alexandra Green at procurement@advancingnutrition.org with subject "RFP No: USAID-AN-055".

The proposals must be prepared in two separate volumes: Technical Proposal and Cost Proposal. The technical and cost proposal must be kept separate. Technical proposals must not refer to pricing data to evaluate the technical proposal strictly on the basis of technical merit.

The written proposal must contain the following information and documentation:

a) Technical Proposal/ Proposed Plan and Approach

The Technical proposal shall describe how the Offeror intends to carry out the Terms of Reference in Attachment 1. It should be concise, specific, complete, and demonstrate a clear understanding of the work

to be undertaken and the responsibilities of all parties involved. It must demonstrate the Offeror's eligibility, as well as their capabilities and expertise in conducting each step of the activity.

The Technical Proposal shall be no more than **7 pages**, including a detailed timeline for completion of the terms of reference, a staffing plan and bio of the team lead. Offeror's shall include only information necessary to provide a clear understanding of the proposed action and the justification for it. Greater detail than necessary, as well as insufficient detail may detract from a proposal's clarity. Assume that the reader is not familiar with the context in which the project will be implemented. Minimize or avoid the use of jargon and acronyms as much as possible. If acronyms or abbreviations are used, include a separate page explaining the terms.

b) Capabilities and Past Performance:

The **Capabilities Statement** shall not exceed **three (3) pages** in length and will be used to evaluate the offeror's organizational, financial, and technical capacity, in relation to the Terms of Reference in Attachment 1. The Capabilities Statement must include but is not limited to: size of the agency, financial resources available to complete this work, staffing competencies and capabilities, past experience performing similar work with other donor organizations, and a company profile and/or brochure.

Additionally, the Offeror must complete and submit the **Past Performance Information** table (see Attachment 3).

The Capabilities Statement and Past Performance Information table will be used to establish the Offeror as a responsible contractor.

c) Cost Proposal Requirements

1. The offeror should submit their most competitive and complete cost proposal (Template here: [LINK](#)).
2. A fixed unit cost and total cost proposal for completion of works as described in the terms of reference (Attachment 1).
3. All costs must be stated in US Dollars with conversion to local currency (please include USD conversion rate).
4. A fixed price for each category of deliverable, each of which will be considered a fixed price budget for that specific segment of work. The price of the sub-contract/PO to be awarded will be an all-inclusive fixed price. No profit, fee or additional costs can be included after the award. All items/ services must be clearly labeled and included in the total offered price.
5. The offeror should submit cost proposal budget narrative.

Cost Proposal Budget Narrative Preparation Instructions

A detailed budget narrative that justifies the costs as appropriate and necessary for the successful completion of proposed activities should be attached to the budget. The budget narrative should clearly describe the project and cost assumptions. [If Applicable: All proposed costs and estimates must be reasonable and allowable in accordance with the US Government's Cost Principles established in 2CFR200, Subpart E.] All proposed costs must be directly applicable to performing the work under the award and budgeted amounts should not exceed the market cost/value of an item or service.

The budget narrative should be of sufficient detail so that someone unfamiliar with your organization or the activity could review and adequately understand and grasp the assumptions, reasonableness and calculation method used.

Budget narrative must be prepared using Microsoft Word software. Supporting information must be provided in adequate detail for conducting a comprehensive analysis.

d) Certifications

The proposal shall be accompanied by all required Certifications in Attachment 2, signed by an authorized official of the offeror.

- a. Representations and Certifications
- b. Certification Regarding Debarment, Suspension, or Proposed Debarment

e) Other (optional)

- a. Letter of reference
- b. Samples of past work

3. AWARD

JSI intends to issue a sub-contract to the offeror who best meet the criteria specified in this RFP and are determined to be responsible and eligible sub-contractor to provide the required goods/services.

4. EVALUATION CRITERIA

Proposals will be evaluated first to ensure that they meet all mandatory requirements as listed above under "Proposal Guidelines". Proposals that fail to meet these requirements will receive no further consideration. A non-responsive proposal to any element may be eliminated from consideration.

Proposals will be evaluated and ranked by a committee on a technical basis according to the criteria below. Those proposals that are considered to be technically acceptable shall then be evaluated in terms of cost

For the purpose of selection, the evaluation will be based on the following weighted point scale (totaling 100 points) of the proposal in its entirety, including, but not limited to, the following:

| No. | Criteria | Points |
|-----|--|--------|
| 1 | Quality of Technical Approach <ul style="list-style-type: none">• Comprehensiveness of proposal approach. Clarity and appropriateness of proposed activity.• Conformity and Responsiveness to Terms of Reference• Technical proposal demonstrates ability to complete deliverables in a realistic timeframe | 50 |
| 2 | Technical Capabilities and Past Performance <ul style="list-style-type: none">• As reflected in completed Capabilities Statement and proposed personnel• Past performance Organizational, financial and technical capabilities and resources to implement this work | 20 |

| | | |
|----------|---|-----|
| 3 | Proposed Costs <ul style="list-style-type: none">• Reasonableness of proposed budget based on scope of activities proposed.• Summary budget, detailed budget, and budget notes included.• Comparative lowest price | 30 |
| | Total | 100 |

4. TERMS OF AWARD

This document is a request for proposals only, and in no way obligates JSI or its donor to make any award. Please be advised that under a fixed price contract the work must be completed within the specified total price. Any expenses incurred in excess of the agreed upon amount in the sub-contract will be the responsibility of the sub-contractor and not that of JSI or its donor. Therefore, the offeror is duly advised to provide its most competitive and realistic proposal to cover all foreseeable expenses related to provide requested goods/services.

All deliverables produced under the future award/sub-contract shall be considered the property of JSI. JSI may choose to award a PO/sub-contract for part of the activities in the RFP. JSI may choose to award a PO/sub-contract to more than one offeror for specific parts of the activities in the RFP.

5. PROPOSAL VALIDITY

The Offeror's technical and cost proposals must remain valid for not less than 120 calendar days after the deadline specified above. Proposals must be signed by an official authorized to bind the Offeror to its provisions.

6. PAYMENT TERMS

JSI payment cycle is net 30 days upon receipt of deliverables, goods/services, inspection and acceptance of goods/services as in compliance with the terms of the award and receipt of vendor invoice. Full cooperation with JSI in meeting the terms and conditions of payment will be given the highest consideration.

7. FINANCIAL RESPONSIBILITY

Offerors which are firms and not individuals must include in the Capabilities Statement that they have the financial viability and resources to complete the proposed activities within the period of performance and under the terms of payment outlined below. JSI reserves the right to request and review the latest financial statements and audit reports of the Offeror as part of the basis of the award.

8. LANGUAGE

The proposal, as well as correspondence and related documents should be in English.

9. SOURCE/NATIONALITY

All goods and services offered in response to this RFQ must meet the source and nationality requirements set forth in United States Code of Federal Regulations, 22 CFR 228. Cuba, Iran, Iraq, Laos, Libya, North Korea, and Syria are prohibited source countries and no goods can be produced or sourced from those countries.

10. NEGOTIATIONS

The Offeror's most competitive proposal is requested. It is anticipated that any award issued will be made solely on the basis of an Offeror's proposal. However, the Project reserves the right to request responses to additional technical, management and cost questions which would help in negotiating and awarding a contract. The Project also reserves the right to conduct negotiations on technical, management, or cost issues prior to the award of a contract. In the event that an agreement cannot be reached with an Offeror the Project will enter into negotiations with alternate Offerors for the purpose of awarding a contract without any obligation to previously considered Offerors.

11. REJECTION OF PROPOSALS

JSI reserves the right to reject any and all proposals received, or to negotiate separately with any and all competing Offerors. The Project also reserves the right to reject any or all proposals received, without explanation.

12. INCURRING COSTS

JSI is not liable for any cost incurred by Offerors during preparation, submission, or negotiation of an award for this RFP. The costs are solely the responsibility of the Offeror.

13. MODIFICATIONS

JSI reserves the right, in its sole discretion, to modify the request, to alter the selection process, to modify or amend the specifications and scope of work specified in this RFQ.

14. CANCELLATION

JSI may cancel this RFP without any cost or obligation at any time until issuance of a contract.

15. CERTIFICATIONS

The proposal shall be accompanied by all required Certifications in Attachment 2, signed by an authorized official of the Offeror.

16. KEY CLAUSES AND PROVISIONS

Key clauses and provisions to be incorporated as applicable into the contract awarded as a result of this solicitation are provided as Attachment 4. The list may not be comprehensive but provides Offerors with the key provisions and clauses to be included.

Attachment 1: Terms of Reference

Service Being Requested: *Request for Proposal for Participatory Implementation Research and Support on Peer Groups*

Estimated Period of Performance: *March 2022 – September 30, 2023*

A. BACKGROUND/RATIONALE

USAID Advancing Nutrition is the Agency’s flagship nutrition project, led by JSI Research & Training Institute, Inc. (JSI), and a diverse group of experienced partners. Launched in September 2018, USAID Advancing Nutrition implements and provides technical support to nutrition interventions across sectors and disciplines for USAID and its partners. The project’s multi-sectoral approach draws together global nutrition experience to design, implement and evaluate programs that address the root causes of malnutrition. Committed to using a systems approach, USAID Advancing Nutrition (USAID AN) strives to sustain positive outcomes by building local capacity, supporting behavior change and strengthening the enabling environment to save lives, improve health, build resilience, increase economic productivity and advance development. (See Attachment 4 for a brief description of the project.)

Nearly all nutrition programs use peer groups to improve the adoption of nutrition behaviors. Groups can contribute to SBC and nutrition outcomes (Kumar et al. 2018), but the SBC assessment of DFSAs conducted by the Food and Nutrition Technical Assistance Project in 2018 identified the variable quality of peer groups as an area for improvement. Few programs use theory or logic models to structure and equip groups. Other challenges for care groups, women’s savings groups, or schools for husbands, include didactic facilitation; insufficient tailored, actionable content beyond informational messages; group segmentation¹⁴; and missed opportunities for social change. USAID Advancing Nutrition seeks to investigate the challenges and collaboratively develop solutions for such peer groups by conducting participatory research with two peer group programs in two contexts.

In consultation with USAID/BHA, USAID AN is conducting implementation research on the nutrition-focused peer groups coordinated by Amalima Loko, a five-year (2020-2025) program designed to improve food security in Zimbabwe through increased food access and sustainable watershed management, funded by the USAID Bureau of Humanitarian Assistance and implemented by Cultivating New Frontiers in Agriculture (CNFA). **To carry out this work, USAID Advancing Nutrition will need support with research tool translation, facilitation of collaborative workshops, data collection, and data analysis.**

B. OBJECTIVE

The specific study objectives are two-fold: to develop a process to work with implementing partners and participants to identify context-specific opportunities to strengthen the quality of peer groups for nutrition programming, and to facilitate a participatory process to design and test transferrable solutions. To support the objective, this study will answer the following research questions:

1. What are the challenges to the quality of peer groups as defined by peer group leaders, members and other key stakeholders?
2. What are feasible ways to improve the quality of peer groups defined by peer group leaders and members?
3. How can peer group leaders' and members' needs and preferences
4. What are the resource requirements and enabling conditions to integrate participant-defined improvements into existing peer groups from the perspective of program participants and implementers?

USAID AN is seeking an in-country research team members to lead and support a participatory research study. The objectives of this support include:

- Serve as Principal Investigator of the research and manage the in-country ethical approval processes.
- Liaise with the local implementing partner to establish a good working relationship and coordinate logistics and communication lines with the partner as well as the research team on USAID Advancing Nutrition.
- Assist with translation and preparation of research tools (interview guides, observation guides, document review guides, etc.) from English into local language and from local language back to English, as needed.
- Attend virtual trainings for the research processes, including qualitative data collection and workshop facilitation.
- Recruit, train and oversee the local data collectors/ team as relevant.
- Facilitate participatory workshops using guides developed by the human-centered design expert on HQ team.
- Conduct individual and group interviews, as well as observations of peer group members and leaders, and prepare detailed notes from interviews and observations.
- Support with data synthesis and analysis
- Support with interpretation (i.e., understanding) of qualitative findings.
- Feed into or review a draft country report slide deck as needed.
- Maintain close coordination with USAID Advancing Nutrition.

C. WORK PLAN - ACTIVITIES/TASKS

The purpose of the support is to assist with on-the-ground research of the Amalima Loko peer group programs' successes and challenges, using participatory, human-centered design research methods.

Using an action research approach, and human-centered, participatory research methods, this research will engage peer group members and leaders, as well as IP staff, to define context-specific challenges and opportunities to strengthen the quality of peer groups for nutrition programming from their perspectives. We will then facilitate a participatory process for group members and leaders to design and test ideas for transferable and reproducible "solutions" or

tangible ways to improve the quality of peer groups and test these solutions in their ongoing peer groups. We will work with IP staff to assess the feasibility and use data to monitor the improvements. Recognizing that each implementing partner has varying commitments, USAID Advancing Nutrition’s research team will adjust the methods, timeline and sample to meet the needs of each study site.

Without knowing the scope of the peer groups being implemented (total number of peer groups, implementation locations, types of peer groups, range of stakeholders, etc.), it is not possible to know the exact sample size at present. However, general guidance for drawing the sample will be to—

- determine lowest administrative unit programmed by the activity (e.g., village)
- in each village determine approximately 5 key stakeholder groups (e.g., peer group leaders, peer group members, community leaders, community health workers, community-based IP staff)
- from each stakeholder group, select 3–5 respondents (e.g., 3 peer group members, 3 community leader, 5 CHWs and 3 community-based IP staff).

The research team will offer additional guidance on how an activity might determine representativeness or decide who is considered a key stakeholder. We estimate that the total sample size (per IP) for discover, define, and develop respondents will be no more than n=75.

Participatory research is proposed with four iterative phases:

| Research Phase | Illustrative Sample Size (per IP) | Illustrative Phase Timeline |
|---|--|--|
| Discover Qualitative research to understand with peer group members, group leaders, stakeholders, and IPs staff about the challenges with quality implementation. | 75** participants We will balance representativeness, saturation, deadlines and humans and financial constraints. | 4-8 weeks, depending on the methods and sample determined with each IP |
| Define Use insights gathered from the research to come to agreement with participants to define the issues to guide next steps. | | 4–8 weeks |

| | | |
|---|--|-----------|
| Develop Then we will facilitate a process for group members, leaders, and staff to develop potential solutions. | | 3–4 weeks |
|---|--|-----------|

**While there is flexibility in the sample size, the research team will work to ensure that the number of peer groups is small enough to support and monitor regularly and intensively, but is also representative of other groups that experience similar challenges.*

During the first two phases, peer group leaders and members with input from staff will identify key challenges to peer group implementation. In the third phase, interlocutors will develop prototypes of solutions based on their prioritized challenges. Group leaders and members will user-test these design interventions, with input from IP staff, to assess their acceptability and feasibility. Learnings from the stage will be documented and presented to key stakeholders, including USAID.

Between April to August 2023, USAID Advancing Nutrition will prepare a country case study or example for each site to summarize and describe the research findings in an easy-to-read format, as well as a slide deck of key findings. In addition, we will develop a full research report that synthesizes findings and recommendations from both sites.

The Offeror will facilitate translation and preparation of research tools, attend qualitative data collection training, set up and conduct group and individual interviews per the protocol, conduct observation of current peer groups, and conduct high quality qualitative data collection. The Offeror will also assist the activity team as they synthesize and analyze qualitative data collected, likely taking a leading role on data synthesis, including outputs from participatory workshops; as well as presentation of the results. The Offeror's familiarity with participatory research methods and Human-Centered Design will be essential.

The Offeror will provide product/services as needed from (on or about) March 20, 2022 to August 23, 2023.

D. PRODUCTS/ SERVICES TO BE INCLUDED IN PROPOSAL

| Line Item | Product/Service Description | Unit | Quant. |
|-----------|--|------------------------------------|-------------------------------|
| 1 | Weekly updates to USAID Advancing Nutrition. | Brief email | Approx. 28 (Over 7 months) |
| 2 | Translate and back translate data collection tools, workshop guides and consent script into local languages | Plan | 1 |
| 3 | Develop plan for and recruit data collectors, and prepare plans and materials for data collector training | Plan | 1 |
| 4 | Support development of and submit the protocol and instruments to in-country ethical review and manage the processes. | Submission | 1 |
| 5 | Prepare a plan for data collection, including the logistics for data collection, in collaboration with the IP | Plan | 1 |
| 6 | Hold data collector training, pre-test, and write summary report with recommendations if relevant | Report | 1 |
| 7 | Develop and implement data quality control, cleaning and management, and security plan. | Plan | 1 |
| 8 | Facilitate participatory workshops using guides developed by the human-centered design expert on HQ team with notes and observations | Workshops | 2 |
| 9 | Conduct individual and group interviews, as well as observations of peer group members and leaders | Interviews/Focus group discussions | Approx. 30 |
| 10 | Develop the codebook for data analysis and oversee the data analysis, including translation as needed | Code books | 1 |
| 11 | Produce field report describing data collection completed, final sample, and any issues faced | Report | 1 |
| 12 | Feed into or review a draft country reporting prepared by USAID Advancing Nutrition on implications and recommendations | Slide deck | 1 |

E. DELIVERABLES AND SCHEDULE

The table below presents the tasks expected, deliverables required, and a schedule for delivery (including due dates). Offerors are requested to propose a payment schedule as part of their cost proposal.

The offeror is expected to submit the following deliverables:

| (Tentative) Due Date | Deliverable Name | Deliverable Description |
|----------------------|--|--|
| April 1, 2022 | Translation of research instruments | Translation and back translation of data collection tools, workshop guides and consent script into local languages |
| April 1, 2022 | Ethical approval MRCZ (or province, as required) | Submit the protocol and instruments to MRCZ for ethical review and manage the processes of questions and responses for final approval. |
| April 15, 2022 | Data collection plan | Recruit and train local data collectors (as relevant). |

| | | |
|--------------------|-----------------------------|--|
| | | Plan for data collection, including the logistics for data collection, in collaboration with the IP |
| April 15, 2022 | Data quality plan | Develop and implement data quality control, cleaning and management, and security plan. |
| May 15, 2022 | Data collection | Conduct individual and group interviews, as well as observations of peer group members and leaders, identifying challenges: <i>phases 1 and 2</i> of the research design |
| June 15, 2022 | Workshops (2) | Facilitate participatory workshops developing solutions using guides developed by the human-centered design expert on HQ team with notes and observations: <i>phase 3</i> of the research design |
| June 15, 2022 | Codebooks and data | Produce codebooks for review with the research team, and cleaned, coded and analyzed data |
| September 30, 2022 | Communication with USAID AN | Weekly updates to USAID Advancing Nutrition Input all updates into a slide deck |

Attachment 2: Certifications

As a condition of accepting a subcontract under this RFP, the Offeror is required to certify to the following mandatory clauses:

2.1. SMALL BUSINESS PROGRAM REPRESENTATIONS (OCT 2014)

(a) *Definitions.* As used in this provision—

“Economically disadvantaged women-owned small business (EDWOSB) concern” means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business concern eligible under the WOSB Program.

“Service-disabled veteran-owned small business concern”—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) “Service-disabled veteran” means a veteran, as defined in [38 U.S.C. 101\(2\)](#), with a disability that is service-connected, as defined in [38 U.S.C. 101\(16\)](#).

“Small business concern” means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and the size standard in paragraph (b) of this provision.

“Small disadvantaged business concern,” consistent with 13 CFR 124.1002, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States, and;

(ii) Each individual claiming economic disadvantage has a net worth not exceeding \$750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13 CFR 124.106) by individuals who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

“Veteran-owned small business concern” means a small business concern—

- (1) Not less than 51 percent of which is owned by one or more veterans (as defined at [38 U.S.C. 101\(2\)](#)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and
- (2) The management and daily business operations of which are controlled by one or more veterans.

“Women-owned small business concern” means a small business concern—

- (1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and
- (2) Whose management and daily business operations are controlled by one or more women.

“Women-owned small business (WOSB) concern eligible under the WOSB Program” (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

(b) Representations.

(1) The offeror represents as part of its offer that it is, is not a small business concern.

(2) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents that it is, is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

(3) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents as part of its offer that it is, is not a women-owned small business concern.

(4) Women-owned small business (WOSB) concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (b)(3) of this provision.] The offeror represents as part of its offer that—

- (i) It is, is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and
- (ii) It is, is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (b)(4)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture: _____.] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(5) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a women-owned small business concern eligible under the WOSB Program in (b)(4) of this provision.] The offeror represents as part of its offer that—

- (i) It is, is not an EDWOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It is, is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (b)(5)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture: _____.] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

(6) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents as part of its offer that it is, is not a veteran-owned small business concern.

(7) [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (b)(6) of this provision.] The offeror represents as part of its offer that it is, is not a service-disabled veteran-owned small business concern.

(8) [Complete only if the offeror represented itself as a small business concern in paragraph (b)(1) of this provision.] The offeror represents, as part of its offer, that—

(i) It is, is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR Part 126; and

(ii) It is, is not a HUBZone joint venture that complies with the requirements of 13 CFR Part 126, and the representation in paragraph (b)(8)(i) of this provision is accurate for each HUBZone small business concern participating in the HUBZone joint venture. [The offeror shall enter the names of each of the HUBZone small business concerns participating in the HUBZone joint venture: _____.] Each HUBZone small business concern participating in the HUBZone joint venture shall submit a separate signed copy of the HUBZone representation.

2.2. CERTIFICATION REGARDING TRAFFICKING IN PERSONS COMPLIANCE PLAN (MAR 2015)

(a) The term “commercially available off-the-shelf (COTS) item,” is defined in the clause of this solicitation entitled “Combating Trafficking in Persons” (FAR clause 52.222-50).

(b) [] This contract will NOT be for supplies, other than commercially available off-the-shelf items, to be acquired outside the United States, or services to be performed outside the United States; or DOES NOT have an estimated value that exceeds \$500,000. Vendor is exempt from this certification requirement.

(c) [] This contract WILL be for supplies, other than commercially available off-the-shelf items, to be acquired outside the United States, or services to be performed outside the United States; and has an estimated value that exceeds \$500,000. Vendor certifies that—

(1) It has implemented a compliance plan to prevent any prohibited activities identified in paragraph (b) of the clause at 52.222-50, Combating Trafficking in Persons, and to monitor, detect, and terminate the contract with a subcontractor engaging in prohibited activities identified at paragraph (b) of the clause at 52.222-50, Combating Trafficking in Persons; and

(2) After having conducted due diligence, either—

- (i) To the best of the Offeror's knowledge and belief, neither it nor any of its proposed agents, subcontractors, or their agents is engaged in any such activities; or
- (ii) If abuses relating to any of the prohibited activities identified in 52.222-50(b) have been found, the Offeror or proposed subcontractor has taken the appropriate remedial and referral actions.

2.3. OTHER REPRESENTATIONS & CERTIFICATIONS

- (a) If the offeror is currently registered in the System for Award Management (SAM), and has completed the Representations and Certifications section of SAM electronically, the offeror may choose to use paragraph (b) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The offeror shall indicate which option applies by checking one of the following boxes:
 - (i) Paragraph (b) applies. Skip to "3" below
 - (ii) Paragraph (b) does not apply and the offeror has completed the individual representations and certifications in the solicitation.
- (b) The offeror has completed the annual representations and certifications electronically via the SAM Web site accessed through <https://www.acquisition.gov>. After reviewing the SAM database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference.
- (c) *Certification Regarding Payments to Influence Federal Transactions (31 U.S.C. 1352)*. By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.
- (d) *Certification Regarding Responsibility Matters (Executive Order 12689)*. The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals—
 - (1) Are, are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;
 - (2) Have, have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: Commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or Commission of embezzlement, theft, forgery, bribery, falsification or

destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property,

(3) [] Are, [] are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) [] Have, [] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds \$3,500 for which the liability remains unsatisfied.

(iii) Taxes are considered delinquent if both of the following criteria apply:

A. *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

B. *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded. (See FAR 52.209-5 for examples)

(e) *Prohibition on Contracting with Inverted Domestic Corporations.*

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) Representation. The offeror represents that—

(i) It [] is, [] is not an inverted domestic corporation; and

(ii) It [] is, [] is not a subsidiary of an inverted domestic corporation.

(f) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that—

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The offeror represents that—

(i) It is [] is not [] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and

that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is [] is not [] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(g) *Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation.* By submission of its offer, the offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

2.4. CERTIFICATION OF OFFEROR

By signature hereon, or on an offer incorporating these Representations and Certifications, the offeror certifies that they are accurate, current, and complete, these Representations and Certifications are binding on the offeror, its successors, transferees, and assignees, and the person or persons whose signatures appear below are authorized to sign these assurances on behalf of the offeror.

Offeror Name _____

Signature _____

Signatory Name _____

Signatory Title _____

Date _____

Attachment 3: Past Performance Information Table

| Item # | Project Name or Contract | Brief Description of Scope of Work and Activities | Geographic Location (country, region, district) | Period of Performance | Total Project Budget or Contract Value (USD\$) | Point of Contact & Contact Details of Funder or Company (Name, Address, Email) |
|---------------|---------------------------------|--|--|------------------------------|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |

INSTRUCTIONS

Complete the above past performance table based on other projects, contracts, or awards for similar work as described in the RFP, Part B: Instructions to Offerors. Preferably provide at least three (3) entries. Add more lines, if applicable.

Attachment 4:

Key Clauses and Provisions

GENERAL TERMS & CONDITIONS

1. **GOODS AND RELATED SERVICES:** The contractor shall deliver the goods and services described on the Purchase Order (PO), of the type, in the quantity, at the delivery date and at the price as indicated on the PO. The quantity of the goods and services shall conform in all respects to the requirements of the PO. All goods (including but not limited to materials, parts, components and sub-assemblies thereof) shall be new, unused, non-remanufactured and non-refurbished.
2. **INSPECTION/ACCEPTANCE:** The Vendor shall tender for acceptance only those items that conform to the requirements of this purchase order. JSI reserves the right to inspect or test any supplies or services that have been tendered for acceptance. JSI may require repair or replacement of nonconforming supplies or re-performance of nonconforming services at no increase in purchase order price. JSI must exercise its post acceptance rights: (1) Within a reasonable period of time after the defect was discovered or should have been discovered; and (2) Before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item. JSI has unilateral authority to determine if the performance results have been met.
3. **INVOICE REQUIREMENTS:** Invoices shall be submitted prior to payment. Each invoice shall identify the Vendor's name, address, invoice number, dates of performance and specify the payment amount. It shall also include a reference to the purchase order number, and specify the goods that have been delivered or the services that have been rendered or the deliverables that have been delivered as a requirement for payment. Upon acceptance of the goods or deliverables by JSI, payment shall be made to the Vendor as per the payment terms and in the currency stated on the purchase order.
4. **TERMINATION FOR CONVENIENCE:** JSI reserves the right to terminate this purchase order, or any part, for its convenience. In the event of such termination, the Vendor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of the purchase order, the Vendor shall be paid a percentage of the purchase order price reflecting the percentage of the work performed prior to the termination.
5. **TERMINATION FOR CAUSE:** JSI reserves the right to terminate this purchase order, or any part, for cause in the event of any defaults by the Vendor, or if the Vendor fails to comply with the terms and conditions of the purchase order, or fails to provide JSI with adequate assurances of future performance. In the event of termination for cause, JSI shall not be liable for any amount of supplies or services not accepted, and the Vendor shall be liable to JSI for any and all rights and remedies provided by law.
6. **WARRANT:** Vendor warrants that the goods and/or services delivered and rendered hereunder conform to the purchase order requirements, are free of latent defects, and are merchantable and fit for use for the particular purpose described in the purchase order (or, if no such purpose is specifically described, for the purposes for which the goods or services, as applicable, are ordinarily used).
7. **CHANGES:** Changes in the terms and conditions of this purchase order may be made only by written amendment issued by JSI.
8. **RISK OF LOSS:** Unless the purchase order specifically provides otherwise, risk of loss or damage to the supplies provided under this purchase order shall remain with the Vendor until, and shall pass to JSI upon delivery of the supplies to JSI at the destination specified in the purchase order. This clause is applicable to goods only.
9. **INDEPENDENT CONTRACTOR:** The relationship between the Parties pursuant to this Purchase Order is that of independent contractors, and nothing contained herein shall be deemed to create a relationship of partners, joint ventures, agent and principal, employer and employee, or any relationship other than that of independent contractors. At no time shall either Party make any commitments or incur any charges or expenses for or in the name of the other Party.

10. **CONFLICT OF INTEREST:** Vendor agrees that there is no conflict of interest in accepting this purchase order, which might affect the ability to conduct fair and useful technical assistance on behalf of JSI.
11. **CONFIDENTIALITY:** The Vendor agrees to treat all information provided by JSI or gathered during the course of providing services as confidential and privileged and to not publish or disseminate such information or otherwise share such information with any third party without the written consent of JSI. The Vendor also agrees to not use such information for any purpose other than the development and implementation of the services provided under this purchase order without the written consent of JSI.
12. **RIGHTS IN WORK PRODUCT:** Vendor agrees that JSI retains the entire right, title and interest in all deliverables, data, and other intellectual property produced by the Vendor under this agreement (collectively "Work Product"). Vendor agrees that the Work Product is specially commissioned and works made-for-hire, and that JSI is deemed the author for copyright purposes. To the extent that any Work Product is not deemed work made-for-hire, Vendor hereby assigns to JSI all its right, title and interest in such Work Product.
13. **PRICES:** The Prices (Unit Prices and extended prices) specified in the purchase order are firm, fixed, all-inclusive total prices including all taxes or duties as may be applicable, and covering performance of all of Vendor's obligations under the purchase order, including, but not limited to, delivery of the goods and/or services in accordance with the purchase order delivery term and performance of all associated and related services.
14. **LIQUIDATED DAMAGES:** Both parties acknowledge that the time fixed for delivery in this Purchase Order is of the essence as well as the difficulty of ascertaining at the time of contracting the precise nature and amount of actual damages JSI will suffer in the event of Vendor's delayed performance. In the event of delay in performance, JSI reserves the right, in addition to any other remedies under this PO, to retain as liquidated damages from any payment due the Vendor an amount equal to one percent (1%) of the cost of the PO for every complete week of delay or a part thereof, reckoning from the time fixed by the PO. The total amount of the liquidated damages shall, however, be limited to ten percent (10%) of the value of the delayed contract. The parties agree that these amounts represent a reasonable estimate of the actual damages anticipated at the time of contracting, and confirm they have been negotiated and agreed upon.
15. **DEBARMENT, SUSPENSION, INELIGIBILITY AND VOLUNTARY EXCLUSION:** The Vendor certifies that neither it nor its principals is presently debarred, suspended, proposed for disbarment, excluded or otherwise disqualified from participation in this transaction by any U.S. Federal Government department or agency, and is not delinquent on any State or Federal tax.
16. **IMPLEMENTATION OF E.O. 13224 - EXECUTIVE ORDER ON TERRORIST FINANCING:** The Vendor is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. This includes individuals or entities that appear on the Specially Designated Nationals and Blocked Persons List maintained by the U.S. Treasury (online at: <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>) or the United Nations Security designation list (online at: http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml). It is the legal responsibility of the Vendor to ensure compliance with these Executive Orders and laws.
17. **MANDATORY DISCLOSURES/ANTI-TRAFFICKING:**
 - a. Vendor must disclose to JSI any credible evidence received that alleges fraud, conflict of interest, bribery, or gratuity violations potentially affecting this purchase order or the Prime Contract/Agreement. Vendor shall not discharge, demote, or otherwise discriminate against any employee as a reprisal for the employee's disclosing such information to JSI, a Member of Congress, or an authorized official of a Federal agency. Disclosures of credible evidence must be submitted to the JSI Code of Conduct Helpline via telephone number 1-855-715-2899 or online at www.jsi.ethicspoint.com.
 - b. JSI is committed to high standards of ethics and integrity including the prohibition of actions that would support trafficking in persons and procedures to prevent such acts and report any violations. As such, JSI's Anti-Trafficking Policy is incorporated into this purchase order. This policy prohibits JSI and its partners, consultants, vendors, and other agents from engaging in trafficking in persons, procurement of commercial sex acts, use of forced labor, and other acts that directly support or advance trafficking in persons. This policy also requires that Vendor immediately report to JSI any information obtained that alleges that any employee, subcontractor, or subcontractor employee has engaged in trafficking in persons, procured commercial sex acts, or used forced labor in the performance of this purchase order. Violations of the JSI Anti-Trafficking Policy must be reported to the JSI Code of Conduct Helpline via telephone number 1-855-715-2899 or online at www.jsi.ethicspoint.com.
 - c. By signing this Agreement, the Vendor confirms that the Vendor has read, understands and agrees to comply

with the JSI/WEI Anti-Trafficking Policy attached or posted at www.jsi.com.

18. **COMPLIANCE WITH LAWS:** Vendor certifies that its employees are authorized to work in the US under US law. Vendor explicitly warrants that it is in compliance with all applicable Federal, state and local laws, as amended, including, as applicable, 41 CFR 60-1.4, 41 CFR 60-250.4, and 41 CFR 60-741.4, with respect to nondiscrimination in employment on the basis of race, religion, color, national origin, or sex, equal opportunity, affirmative action, employment of disabled veterans, and veterans of the Vietnam era, and employment of the handicapped. If this is a Purchase Order for services, Vendor also shall not discriminate against any of the intended beneficiaries of the program for which services are provided, such as, but not limited to, by withholding, adversely impacting, or denying equitable access to the benefits provided through the program on the basis of any factor not expressly stated in this agreement.
19. **ANTI-LOBBYING:** The Vendor, by signing this purchase order, hereby certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress on its behalf in connection with the awarding of this purchase order.
20. **REMEDIES:** Violation of any of the terms and conditions of this agreement constitutes grounds for termination of the assignment and may result in the Vendor being barred from future assignments with JSI. The exercise of these rights does not limit JSI's right to also seek any and all other legal remedies.
21. **INDEMNIFICATION:** The Vendor shall indemnify and hold JSI harmless from any claim, suit, loss, damage, cost or expenses (including reasonable attorneys' fees) arising out of or in connection with the Vendor's negligence, willful misconduct, breach of this agreement, or other legal wrong-doing in any way connected with activities under this Agreement.
22. **DISPUTES:** In the event of any claims or disputes arising from or relating to this Purchase Order, the parties shall use their best efforts to settle the claims or disputes. To this effect, they shall consult and negotiate with each other in good faith and, recognizing their mutual interests, attempt to reach a just and equitable solution satisfactory to both parties. If they fail to reach such a solution within sixty (60) days, either Party may refer the matter to arbitration, which shall be the exclusive method of resolving such disputes. The arbitration shall be conducted in Boston, Massachusetts or, if JSI determines at its sole discretion it would be more convenient, in the country of performance. The arbitration shall be administered by the American Arbitration Association's International Centre for Dispute Resolution in accordance with its International Arbitration Rules before a single arbitrator appointed in accordance with such rules. The results of arbitration shall be final and binding on the Parties and shall be in lieu of any other remedy. Judgment may be entered upon the award in any court of competent jurisdiction.
23. **FORCE MAJEURE:** Neither party shall be liable in damages for any default in performing hereunder if such default is caused by a force majeure event, including, but not limited to Acts of God, Government restrictions, wars, insurrections and/or any other cause beyond the reasonable control of the party whose performance is affected.
24. **GENERAL:**
 - a. This Purchase Order is the sole and entire agreement between the parties relating to the subject matter hereof, and supersedes all prior understandings, agreements, and documentation relating to the subject matter hereof. This Purchase Order may be amended only by an instrument executed by the authorized representatives of both parties.
 - b. Every provision of this Purchase Order is intended to be severable. If any term or provision of this agreement is illegal or invalid for any reason, the illegality or invalidity shall not affect the legality or validity of the remainder of this Purchase Order, and all other provisions of this agreement shall remain in full force and effect.
 - c. This Purchase Order shall be interpreted in accordance with the substantive law of the Commonwealth of Massachusetts.

FUNDER REQUIRED CLAUSES

1. **NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE.**
 - (a) This contract incorporates one or more clauses by reference. When applicable, these clauses are given the same force and effect as if they were given in full text. Upon request, JSI will make their full text available. Also, the full text of a clause may be accessed electronically at these address(es):

<http://farsite.hill.af.mil/vffara.htm>

<https://www.acquisition.gov/far/current/html/FARTOCP52.html>

http://www.usaid.gov/sites/default/files/documents/1868/aidar_0.pdf

- (b) For purposes of the those clauses that provide for rights, obligations and procedures effecting the Government's rights and JSI's obligations under the prime agreement, references to the "Contractor" shall mean "Vendor" and "Contract" shall mean "Purchase Order;" references to the "Government" shall mean the "Government and JSI", "the Contracting Officer" shall mean the "Contracting Officer and JSI." In all other instances, references to the "Government" shall mean "JSI;" references to the "Government Contracting Officer" shall mean the "JSI."

Federal Acquisition Regulation (48 CFR Chapter 1)

| Number | Title | Date |
|-----------|---|----------|
| 52.202-1 | Definitions. | NOV 2013 |
| 52.203-3 | Gratuities. | APR 1984 |
| 52.203-5 | Covenant against Contingent Fees. | MAY 2014 |
| 52.203-6 | Restriction on Subcontractor Contract Sales to Government. | SEP 2006 |
| 52.203-7 | Anti-Kickback Procedures. | MAY 2014 |
| 52.203-8 | Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity. | MAY 2014 |
| 52.203-10 | Price or Fee Adjustment for Illegal or Improper Activity. | MAY 2014 |
| 52.203-12 | Limitation on Payments to Influence Certain Federal Transactions. | OCT 2010 |
| 52.203-13 | Contractor Code of Business Ethics and Conduct. | OCT 2015 |
| 52.203-14 | Display Hotline Poster(s). | OCT 2015 |
| 52.203-16 | Preventing Personal Conflicts of Interest. | DEC 2011 |
| 52.203-17 | Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights. | APR 2014 |
| 52.203-19 | Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements. | JAN 2017 |
| 52.204-21 | Basic Safeguarding of Covered Contractor Information Systems. | JUN 2016 |
| 52.204-23 | Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab or Other Covered Entities. | JUL 2018 |
| 52.209-6 | Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. | OCT 2015 |
| 52.209-10 | Prohibition on Contracting with Inverted Domestic Corporations. | NOV 2015 |
| 52.209-13 | Violation of Arms Control Treaties or Agreements – Certification. | JUL 2018 |
| 52.215-10 | Price Reduction for Defective Certified Cost or Pricing Data. | AUG 2011 |
| 52.215-11 | Price Reduction for Defective Certified Cost or Pricing Data – Modifications. | AUG 2011 |
| 52.215-14 | Integrity of Unit Prices. | OCT 2010 |
| 52.215-19 | Notification of Ownership Changes. | OCT 1997 |
| 52.219-8 | Utilization of Small Business Concerns. | NOV 2016 |
| 52.222-17 | Nondisplacement of Qualified Workers. | MAY 2014 |
| 52.222-20 | Contracts for Materials, Supplies, Articles, and Equipment Exceeding \$15,000. | MAY 2014 |
| 52.222-21 | Prohibition of Segregated Facilities. | APR 2015 |
| 52.222-26 | Equal Opportunity. | SEP 2016 |
| 52.222-29 | Notification of Visa Denial. | APR 2015 |
| 52.222-35 | Equal Opportunity for Veterans. | OCT 2015 |
| 52.222-36 | Equal Opportunity for Workers with Disabilities. | JUL 2014 |
| 52.222-37 | Employment Reports on Veterans. | FEB 2016 |

| | | |
|-----------|---|----------|
| 52.222-40 | Notification of Employee Rights under the National Labor Relations Act. | DEC 2010 |
| 52.222-50 | Combating Trafficking in Persons. | MAR 2015 |
| 52.222-54 | Employment Eligibility Verification. | OCT 2015 |
| 52.223-6 | Drug Free Work Place. | MAY 2011 |
| 52.223-18 | Encouraging Contractor Policies to Ban Text Messaging While Driving. | AUG 2018 |
| 52.225-13 | Restrictions on Certain Foreign Purchases. | JUN 2008 |
| 52.227-1 | Authorization and Consent. | DEC 2007 |
| 52.227-14 | Rights in Data – General. | MAY 2014 |
| 52.228-3 | Worker’s Compensation Insurance (Defense Base Act). | JUL 2014 |
| 52.228-7 | Insurance – Liability to Third Persons. | MAR 1996 |
| 52.230-2 | Cost Accounting Standards. | OCT 2015 |
| 52.230-6 | Administration of Cost Accounting Standards. | JUN 2010 |
| 52.232-18 | Availability of Funds. | APR 1984 |
| 52.232-23 | Assignment of Claims. | MAY 2014 |
| 52.232-25 | Prompt Payment. | JAN 2017 |
| 52.232-25 | Prompt Payment. (JAN 2017) - Alternate I. | FEB 2002 |
| 52.233-3 | Protest after Award. | AUG 1996 |
| 52.233-3 | Protest after Award. (AUG 1996) - Alternate I. | JUN 1985 |
| 52.242-13 | Bankruptcy. | JUL 1995 |
| 52.244-5 | Competition in Subcontracting. | DEC 1996 |
| 52.244-6 | Subcontracts for Commercial Items. | JAN 2017 |
| 52.245-1 | Government Property. | JAN 2017 |
| 52.245-9 | Use and Charges. | APR 2012 |
| 52.247-63 | Preference for U.S.-Flag Air Carriers. | JUN 2003 |
| 52.247-64 | Preference for Privately Owned U.S.-Flag Commercial Vessels. | FEB 2006 |
| 52.253-1 | Computer Generated Forms. | JAN 1991 |

USAID Regulations (AIDAR) (48 CFR Chapter 7)

| Number | Title | Date |
|---------------|---|-------------|
| 752.202-1 | Definitions | JAN 1990 |
| 752.209-71 | Organizational Conflicts of Interest Discovered after Award. | JUN 1993 |
| 752.211-70 | Language and Measurement. | JUN 1992 |
| 752.219-8 | Utilization of Small Business Concerns and Small Disadvantaged Business Concerns. | MAR 2015 |
| 752.222-70 | USAID Disability Policy. | DEC 2004 |
| 752.222-71 | Nondiscrimination. | JUN 2012 |
| 752.225-70 | Source and Nationality Requirements. | FEB 2012 |
| 752.228-3 | Worker’s Compensation Insurance (Defense Base Act). | DEC 1991 |
| 752.228-7 | Insurance – Liability to Third Persons. | JUL 1997 |
| 752.228-70 | Medical Evacuation (MEDEVAC) Services. | JUL 2007 |
| 752.229-70 | Federal, State and Local Taxes. | |
| 752.7009 | Marking. | JAN 1993 |
| 752.7012 | Protection of the Individual as a Research Subject. | AUG 1995 |
| 752.7034 | Acknowledgement and Disclaimer. | DEC 1991 |

| | | |
|----------|--|----------|
| 752.7037 | Child Safeguarding Standards. | AUG 2016 |
| 752.7038 | Nondiscrimination against End-Users of Supplies or Services. | OCT 2016 |

2. CONDOMS (ACQUISITION) (SEPTEMBER 2014)

Information provided about the use of condoms as part of projects or activities that are funded under this contract shall be medically accurate and shall include the public health benefits and failure rates of such use and shall be consistent with USAID's fact sheet entitled, "USAID HIV/STI Prevention and Condoms." This fact sheet may be accessed at: <http://www.usaid.gov/sites/default/files/documents/1864/CondomSTIIssueBrief.pdf>

The Contractor agrees to incorporate the substance of this clause in all subcontracts under this contract for HIV/AIDS activities

3. PROHIBITION ON THE PROMOTION OR ADVOCACY OF THE LEGALIZATION OR PRACTICE OF PROSTITUTION OR SEX TRAFFICKING (SEPTEMBER 2014)

(a) This contract is authorized under the United States Leadership Against HIV/AIDS, Tuberculosis, and Malaria Act of 2003 (Pub.L. No. 108-25), as amended. This Act enunciates that the U.S. Government is opposed to prostitution and related activities, which are inherently harmful and dehumanizing, and contribute to the phenomenon of trafficking in persons. The Contractor shall not use any of the funds made available under this contract to promote or advocate the legalization or practice of prostitution or sex trafficking. Nothing in the preceding sentence shall be construed to preclude the provision to individuals of palliative care, treatment, or post-exposure pharmaceutical prophylaxis, and necessary pharmaceuticals and commodities, including test kits, condoms, and, when proven effective, microbicides.

(b) (1) Except as provided in (b)(2), by its signature of this contract or subcontract for HIV/AIDS activities, a non-governmental organization or public international organization awardee/subawardee agrees that it is opposed to the practices of prostitution and sex trafficking.

(2) The following organizations are exempt from (b)(1):

- i. The Global Fund to Fight AIDS, Tuberculosis, and Malaria; the World Health Organization; the International AIDS Vaccine Initiative; and any United Nations agency.
- ii. U.S. non-governmental organization recipients/subrecipients and contractors/subcontractors
- iii. Non-U.S. Contractors and subcontractors are exempt from (b)(1) if the contract or subcontract is for commercial items and services as defined in FAR 2.101, such as pharmaceuticals, medical supplies, logistics support, data management, and freight forwarding.

(3) Notwithstanding section (b)(2)(iii), not exempt from (b)(1) are non-U.S. Contractors and subcontractors that implement HIV/AIDS programs under this contract or subcontract by:

- i. providing supplies or services directly to the final populations receiving such supplies or services in host countries;
- ii. providing technical assistance and training directly to host country individuals or entities on the provision of supplies or services to the final populations receiving such supplies and services; or
- iii. providing the types of services listed in FAR 37.203(b)(1)-(6) that involve giving advice about substantive policies of a recipient, giving advice regarding the activities referenced in (i) and (ii), or making decisions or functioning in a recipient's chain of command (e.g., providing managerial or supervisory services approving financial transactions, personnel actions).

(c) The following definitions apply for purposes of this provision:

"Commercial sex act" means any sex act on account of which anything of value is given to or received by any person.

"Prostitution" means procuring or providing any commercial sex act and the "practice of prostitution" has the same meaning.

"Sex trafficking" means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act. 22 U.S.C. 7102(9).

(d) The Contractor shall insert this provision in all subcontracts for HIV/AIDS activities.

(e) Any violation of this provision will result in the immediate termination of this award by USAID.

(f) This provision does not affect the applicability of FAR 52.222-50 to this contract.

4. AIDAR 752.7005 SUBMISSION REQUIREMENTS FOR DEVELOPMENT EXPERIENCE DOCUMENTS (SEPTEMBER 2013)

(a) Subcontract Reports and Information/Intellectual Products.

- (1) JSI is required by the terms of the Prime Contract to submit to USAID's Development Experience Clearinghouse (DEC) reports and information products which describe, communicate or organize program/project development assistance activities, methods, technologies, management, research, results and experience. This includes applicable reports and information products produced by the Subcontractor.
- (2) The Subcontractor shall submit one electronic copy of applicable reports and information products to JSI who will submit this documentation to the DEC within thirty (30) days of receiving the Contracting Officer's Representative's approval.
- (3) These reports and information products include: assessments, evaluations, studies, technical and periodic reports, annual and final reports, and development experience documents (defined as documents that: (i) Describe the planning, design, implementation, evaluation, and results of development assistance; and ii) Are generated during the life cycle of development assistance programs or activities.) The Subcontractor must also submit copies of information products including training materials, publications, databases, computer software programs, videos, and other intellectual deliverable materials required under the Contract Schedule.
- (4) The following information is not to be submitted:
 - (i) Time-sensitive materials such as newsletters, brochures, or bulletins.
 - (ii) The Subcontractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information.
- (5) Within twenty (20) calendar days after completion of the Subcontract, the Subcontractor must submit to JSI for submission to the DEC any reports that have not been previously submitted and an index of all reports and information/intellectual products referenced in paragraph (a)(3) of this clause.

(b) Submission requirements. The Subcontractor must review the DEC Web site for the most up-to-date submission instructions, including document formatting and the types of documents to be submitted. The submission instructions can be found at: <https://dec.usaid.gov>. All actual submissions to the DEC will be done by JSI.

(1) Standards.

- (i) Material must not include financially sensitive information or personally identifiable information (PII) such as social security numbers, home addresses, and dates of birth. Such information must be removed prior to submission.
 - (ii) All submissions must conform to current USAID branding requirements.
 - (iii) Subcontract reports and information/intellectual products can be submitted in either electronic (preferred) or paper form. Electronic documentation must comply with Section 508 of the Rehabilitation Act of 1973.
 - (iv) The electronic submissions must consist of only one electronic file, which comprises the complete and final equivalent of the paper copy. In the case of databases and computer software the submissions must also include necessary descriptive information, e.g., special backup or data compression routines, software used for storing/retrieving submitted data, or program installation instructions.
 - (v) Electronic documents must be in one of the National Archives and Records Administration (NARA)-approved formats as described in NARA guidelines related to the transfer of permanent E-records. (See <http://www.archives.gov/records-mgmt/initiatives/transfer-to-nara.html>).
- (2) Essential bibliographic information. Descriptive information is required for all Subcontractor products submitted. The title page of all reports and information products must include the Subcontract and Prime Contract numbers, Subcontractor and Prime Contractor names, name of the USAID Contracting Officer's Representative, the publication or issuance date of the document, document title (if non-English, provide

an English translation of the title), author name(s), and development objective or activity title (if non-English, provide a translation) and associated number, and language of the document (if non-English). In addition, all hard copy materials submitted in accordance with this clause must have, attached as a separate cover sheet, the name, organization, address, telephone number, fax number, and internet address of the submitting party.

5. ADS 302.3.5.19 USAID-FINANCED THIRD-PARY WEB SITES (SEPTEMBER 2017)

(a) Definitions:

“Third-party web sites”

Sites hosted on environments external to USAID boundaries and not directly controlled by USAID policies and staff, except through the terms and conditions of a contract. Third-party Web sites include project sites.

(b) The Subcontractor must adhere to the following requirements when developing, launching, and maintaining a third-party Web site funded by USAID for the purpose of meeting the project implementation goals:

- (1) Prior to Web site development, the Subcontractor must provide information as required in Section C. Performance Work Statement of the Prime Contract (including a copy of the Subcontractor’s privacy policy) to the Contracting Officer’s Representative (COR) for USAID’s Bureau for Legislative and Public Affairs (LPA) evaluation and approval through JSI USAID Advancing Nutrition Project Director. The Subcontractor must notify the USAID COR through JSI USAID Advancing Nutrition Project Director of the Web site URL as far in advance of the site’s launch as possible and must not launch the Web site until USAID COR approval has been provided through JSI. The Subcontractor must provide the JSI USAID Advancing Nutrition Project Director with any changes to the privacy policy for the duration of the Subcontract.
- (2) The Subcontractor must collect only the amount of information necessary to complete the specific business need as required by statute, regulation, or Executive Order.
- (3) The Subcontractor must comply with Agency branding and marking requirements comprised of the USAID logo and brand mark with the tagline “from the American people,” located on the USAID Web site at www.usaid.gov/branding, and USAID Graphics Standards manual at <http://www.usaid.gov>.
- (4) The Web site must be marked on the index page of the site and every major entry point to the Web site with a disclaimer that states:

"The information provided on this Web site is not official U.S. Government information and does not represent the views or positions of the U.S. Agency for International Development or the U.S. Government."
- (5) The Web site must provide persons with disabilities access to information that is comparable to the access available to others. As such, all site content must be compliant with the requirements of the Section 508 amendments to the Rehabilitation Act.
- (6) The Subcontractor must identify and provide to the USAID COR through JSI USAID Advancing Nutrition Project Director or designee, in writing, the contact information for the information security point of contact. The Subcontractor is responsible for updating the contact information whenever there is a change in personnel assigned to this role.
- (7) The Subcontractor must provide adequate protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted on the Web sites. To minimize security risks and ensure the integrity and availability of information, the Subcontractor must use sound: system/software management; engineering and development; and secure-coding practices consistent with USAID standards and information security best practices. Rigorous security safeguards, including but not limited to, virus protection; network intrusion detection and prevention programs; and vulnerability management systems must be implemented and critical security issues must be resolved as quickly as possible or within thirty (30) days. Contact the USAID Chief Information Security Officer (CISO) through JSI for specific standards and guidance.
- (8) The Subcontractor must conduct periodic vulnerability scans, mitigate all security risks identified during such scans, and report subsequent remediation actions to USAID CISO and COR through JSI USAID Advancing Nutrition Project Director within thirty (30) workdays from the date vulnerabilities are identified. The report must include disclosure of

the tools used to conduct the scans. The Subcontractor will be responsible for taking the necessary remediation action and reporting to USAID through JSI as specified above.

- (c) For general information, agency graphics, metadata, privacy policy, and 508 compliance requirements, refer to <http://www.usaid.gov>.

6. SUBMISSION OF DATASETS TO THE DEVELOPMENT DATA LIBRARY (DDL) (OCTOBER 2014)

- (a) Definitions. For the purpose of submissions to the DDL:

- (1) "Dataset" is an organized collection of structured data, including data contained in spreadsheets, whether presented in tabular or non-tabular form. For example, a Dataset may represent a single spreadsheet, an extensible mark-up language (XML) file, a geospatial data file, or an organized collection of these. This requirement does not apply to aggregated performance reporting data that the Subcontractor submits to a USAID portfolio management system either directly or through JSI or to unstructured data, such as email messages, PDF files, PowerPoint presentations, word processing documents, photos and graphic images, audio files, collaboration software, and instant messages. Neither does the requirement apply to the Subcontractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information. Datasets submitted to the DDL will generally be those generated with USAID resources and created in support of Intellectual Work that is uploaded to the Development Experience Clearinghouse (DEC) (see AIDAR 752.7005 "Submission Requirements for Development Experience Documents").
- (2) "Intellectual Work" includes all works that document the implementation, monitoring, evaluation, and results of international development assistance activities developed or acquired under this award, which may include program and communications materials, evaluations and assessments, information products, research and technical reports, progress and performance reports required under this award (excluding administrative financial information), and other reports, articles and papers prepared by the Subcontractor under the award, whether published or not. The term does not include the Subcontractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information.

- (b) Submissions to the Development Data Library (DDL)

- (1) The Subcontractor must submit to JSI for further submission to the Development Data Library (DDL) in a machine-readable, non-proprietary format, a copy of any Dataset created or obtained in performance of this award, including Datasets produced by a subcontractor at any tier. The submission must include supporting documentation describing the Dataset, such as code books, data dictionaries, data gathering tools, notes on data quality, and explanations of redactions.
- (2) Unless otherwise directed by the USAID CO or the COR through JSI USAID Advancing Nutrition Project Director, the Subcontractor must submit the Dataset and supporting documentation within thirty (30) calendar days after the Dataset is first used to produce an Intellectual Work or is of sufficient quality to produce an Intellectual Work. Within thirty (30) calendar days after Work Order completion, the Subcontractor must submit to JSI for further submission to the DDL any Datasets and supporting documentation that have not previously been submitted to JSI for further submission to the DDL, along with an index of all Datasets and Intellectual Work created or obtained under the award. The Subcontractor is not required to submit the data to JSI for submission to the DDL, when, in accordance with the terms and conditions of this award, Datasets containing results of federally funded scientific research are submitted to a publicly accessible research database. However, the Subcontractor must submit a notice to JSI providing details on where and how to access the data. The direct results of federally funded scientific research must be reported no later than when the data are ready to be submitted to a peer-reviewed journal for publication, or no later than five (5) calendar days prior to the conclusion of the Work Order, whichever occurs earlier.
- (3) The Subcontractor must submit the Datasets following the submission instructions and acceptable formats found at www.usaid.gov/data.
- (4) The Subcontractor must ensure that any Dataset submitted to JSI for further submission to the DDL does not contain any proprietary or personally identifiable information, such as social security numbers, home addresses, and dates of birth. Such information must be removed prior to submission.

- (c) The Subcontractor must not submit classified data to JSI for further submission the DDL.

7. COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973, AS AMENDED

- (a) The Subcontractor must provide a comprehensive list of all offered specific electronic and information technology (EIT) products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR Part 1194. The Subcontractor must clearly indicate where this list with full details of compliance can be found (e.g., vendors or other exact web page location). The Subcontractor must ensure that the list is easily accessible by typical users beginning five calendar days after award. The Subcontractor must maintain this detailed listing of compliant products for the full Subcontract term, including all forms of extensions, and must ensure that it is current within three calendar days of changes to its product line.
- (b) For every EIT product accepted under this Subcontract by the Government that does not comply with 36 CFR Part 1194, the Subcontractor must make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral, on either the planned refresh cycle of the product or service, or on the contract renewal date, whichever shall occur first.

8. CLOUD COMPUTING (APRIL 2018)

- (a) Definitions. As used in this special contract requirement:

"Cloud Computing" means a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This includes other commercial terms, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. It also includes commercial offerings for software-as-a-service, infrastructure-as-a-service, and platform-as-a-service.

"Cloud Service Provider" or CSP means a company or organization that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

"Federal Information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government, in any medium or form. (OMB A-130)

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual [Committee on National Security Systems Instruction (CNSSI) 4009].

"Information Security Incident" means 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.

"Privacy Incident" means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of Personally Identifiable Information (PII), whether in electronic or paper format.

"Spillage" means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited (i.e., authorized) for the applicable security level of the data or information.

"Penetration Testing" means security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. (NIST SP 800-115)

"Third Party Assessment Organizations" means an organization independent of the organization whose IT system is being assessed. They are required to meet the ISO/IEC 17020:1998 standards for independence and managerial competence and meet program requirements for technical FISMA competence through demonstrated expertise in assessing cloud-based solutions.

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The definition of PII is not anchored to any single category of information or technology.

Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual. PII examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PII can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining PII for USAID purposes, the term “individual” refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

(b) **Applicability:** This special contract requirement applies to the Subcontractor and all personnel providing support under this Subcontract (hereafter referred to collectively as “Subcontractor”) and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) **Limitations on access to, use and disclosure of, Federal information.**

- (1) The Subcontractor shall not access, use, or disclose Federal information unless specifically authorized by the terms of this Subcontract issued hereunder.
 - (i) If authorized by the terms of this Subcontract issued hereunder, any access to, or use or disclosure of, Federal information shall only be for purposes specified in this Subcontract.
 - (ii) The Subcontractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.
 - (iii) These access, use, and disclosure prohibitions and obligations shall remain effective beyond the expiration or termination of this Subcontract.
- (2) The Subcontractor shall use related Federal information only to manage the operational environment that supports the Federal information and for no other purpose unless otherwise permitted with the prior written approval of the USAID Contracting Officer through JSI.

(d) **Records Management and Access to Information.**

- (1) The Subcontractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with capabilities such as those identified in the provisions of this Subcontract and National Archives and Records Administration (NARA) retention policies.
- (2) Upon request by JSI, the Subcontractor shall deliver to the USAID Contracting Officer through JSI USAID Advancing Nutrition Project Director or designee all Federal information, including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by JSI USAID Advancing Nutrition Project Director or designee in support of government compliance requirements to include but not limited to Freedom of Information Act, Privacy Act, e-Discovery, e-Records and legal or security investigations.
- (3) The Subcontractor shall retain and maintain all Federal information in accordance with records retention provisions negotiated by the terms of the Subcontract and in accordance with USAID records retention policies.
- (4) The Subcontractor shall dispose of Federal information in accordance with the terms of the Subcontract and provide the confirmation of disposition to the USAID Contracting Officer through JSI USAID Advancing Nutrition Project Director or designee in accordance with Subcontract closeout procedures.

(e) **Notification of Third Party Access to Federal Information:** The Subcontractor shall notify the Government and JSI immediately of any requests from a third party for access to Federal information or, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or Local agency, that could result in the disclosure of any Federal information to a third party. The Subcontractor shall cooperate with the Government to take all measures to protect Federal information, from any loss or unauthorized disclosure that might reasonably result from the execution of any such request, warrant, seizure, subpoena, or similar legal process.

- (f) Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Subcontractor's discovery of a spillage or security incident involving classified information, the Subcontractor shall immediately (within thirty (30) minutes) notify CIO-HELPDESK@usaid.gov, the Office of Security at SECinformationsecurity@usaid.gov, and JSI USAID Advancing Nutrition Project Director or designee to correct the spillage or information security incident in compliance with agency-specific instructions. The Subcontractor will also notify the USAID Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer through JSI. The Subcontractor will abide by USAID instructions on correcting such a spill or information security incident. For all spills and information security incidents involving unclassified and/or SBU information, the protocols outlined above in section (g) and (h) below shall apply.

(g) Information Security Incidents.

- (1) Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the information security incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.

- (i) Subcontractor employees must report via e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than thirty (30) minutes, after becoming aware of the Incident, at: CIO-HELPDESK@usaid.gov, and JSI USAID Advancing Nutrition Project Director or designee regardless of day or time, as well as the USAID Contracting Officer and Contracting Officer's Representative, the Contractor Facilities Security Officer through JSI USAID Advancing Nutrition Project Director or designee.

Subcontractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Subcontractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

- (ii) The Subcontractor must provide any supplementary information or reports related to a previously reported information security incident directly to CIO-HELPDESK@usaid.gov, upon request with a copy to JSI USAID Advancing Nutrition Project Director or designee. Correspondence must include related ticket number(s) as provided by the USAID Service Desk with the subject line "Action Required: Potential Security Incident."

- (h) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information, and can result in the loss of the public's trust and confidence in the Agency's ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Subcontractor employees must report by e-mail all Privacy Incidents to the USAID Service Desk immediately (within thirty (30) minutes), after becoming aware of the Incident, at: CIO-HELPDESK@usaid.gov, regardless of day or time, and JSI USAID Advancing Nutrition Project Director or designee, as well as the USAID Contracting Officer or Contracting Officer's Representative, the Contractor Facilities Security Officer through JSI. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read "Action Required: Potential Privacy Incident."

- (i) Information Ownership and Rights: USAID information stored in a cloud environment remains the property of USAID, not the Subcontractor or cloud service provider (CSP). USAID retains ownership of the information and any media type that stores Federal information. The CSP shall only use the Federal information for purposes explicitly stated in the Prime Contract. Furthermore, the cloud service provider shall export Federal information in a machine-readable and non-proprietary format that USAID requests at the time of production, unless the parties agree otherwise.

(j) Security Requirements:

- (1) The Subcontractor shall adopt and maintain administrative, technical, operational, and physical safeguards and controls that meet or exceed requirements contained within the Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline, current standard for NIST 800-53 (Security and Privacy Controls for Federal Information Systems) and Organizations, including Appendix J, and FedRAMP Continuous Monitoring Requirements for the security level and services being provided, in accordance with the security categorization or impact level as defined by the government based on the Federal Information Processing Standard

(FIPS) Publication 199 (FIPS-199).

- (2) The Subcontractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the security assessment and authorization (SA&A) is based on the system's complexity and security categorization. The Subcontractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at <https://www.FedRAMP.gov>.
- (3) The Subcontractor must support SA&A activities to include assessment by an accredited Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan. The Subcontractor must make available to the USAID Contracting Officer, the most current, and any other, Security Assessment Reports for consideration as part of the Subcontractor's overall Systems Security Plan.
- (4) The Government reserves the right to perform penetration testing or request Penetration Testing by an independent source. If the Government exercises this right, the Subcontractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems, web applications, databases, 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 Federal information for vulnerabilities.
- (5) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Subcontractor's implementation as documented in the Security Assessment Report must be tracked by the Subcontractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.
- (6) The Subcontractor is responsible for mitigating all security risks found during SA&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within thirty (30) calendar days and all moderate risk vulnerabilities must be mitigated within sixty (60) calendar days from the date vulnerabilities are formally identified. USAID may revoke an ATO for any system if it is determined that the system does not comply with USAID standards or presents an unacceptable risk to the Agency. The Government will determine the risk rating of vulnerabilities.
 - (7) The Subcontractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements and to allow for appropriate risk decisions for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The Subcontractor must make appropriate personnel available for interviews and provide all necessary documentation during this review and as necessary for continuous monitoring activities.
- (k) Privacy Requirements: Cloud Service Provider (CSP) must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect Personally Identifiable Information (PII) about individuals that will be collected and maintained by the Subcontractor solution. The Subcontractor responsibilities include full cooperation for any request for disclosure, subpoena, or other judicial process seeking access to records subject to the Privacy Act of 1974.
- (l) Data Location: The Subcontractor must disclose the data server locations where the Agency data will be stored as well as the redundant server locations. The Subcontractor must have prior Agency approval obtained through JSI to store Agency data in locations outside of the United States.
 - (m) Terms of Service (ToS): The Subcontractor must disclose any requirements for terms of service agreements and clearly define such terms prior to subcontract award. All ToS provisions regarding controlling law, jurisdiction, and indemnification must align with Federal statutes, policies, and regulations.
 - (n) Service Level Agreements (SLAs): The Subcontractor must be willing to negotiate service levels with USAID through JSI; clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have been resolved or mitigated. Additionally, at USAID's request, the Subcontractor must submit reports or provide a dashboard where USAID can continuously verify that service levels are being met. Where SLAs fail to be met, USAID may assess monetary penalties or service credit.
 - (o) Trusted Internet Connection (TIC): The Subcontractor must route all USAID traffic through the TIC.

(p) Forensics, Freedom of Information Act (FOIA), Electronic Discovery, or Additional Information Requests: The Subcontractor must allow USAID access required to retrieve information necessary for FOIA and Electronic Discovery activities, as well as, forensic investigations for both criminal and non-criminal purposes without their interference in these activities. USAID may negotiate roles and responsibilities for conducting these activities in agreements outside of this Subcontract.

- (1) The Subcontractor must ensure appropriate forensic tools can reach all devices based on an approved timetable.
- (2) The Subcontractor must not install forensic software or tools without the permission of USAID obtained through JSI.
- (3) The Subcontractor, in coordination with USAID Bureau for Management, Office of The Chief Information Officer (M/CIO)/ Information Assurance Division (IA), must document and preserve data required for these activities in accordance with the terms and conditions of the Subcontract.
- (4) The Subcontractor, in coordination with USAID M/CIO/IA, must clearly define capabilities, procedures, roles and responsibilities and tools and methodologies for these activities.

(q) The Subcontractor shall include the substance of this special contract requirement, including this paragraph (q), in all subcontracts, including subcontracts for commercial items.

9. INFORMATION TECHNOLOGY APPROVAL (APRIL 2018) (DEVIATION NO. M/OAA-DEV-FAR-18-2C)

(a) Definitions. As used in this Subcontract –

“Information Technology” means

- (1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where
 - (2) such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.
 - (3) The term " information technology" 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 provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.
 - (4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (OMB M-15-14)
- (b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval through JSI of contracts or interagency agreements for information technology or information technology services.
- (c) The approved information technology and/or information technology services are specified in the Schedule of this subcontract. The Subcontractor must not acquire additional information technology without the prior written approval of the USAID Contracting Officer through JSI as specified in this clause.
- (d) Request for Approval Requirements:
- (1) If the Subcontractor determines that any information technology in addition to that information technology specified in the Schedule will be necessary to meet the Government’s requirements or to facilitate activities in the statement of work, the Subcontractor must request prior written approval from the USAID Contracting Officer through JSI.
 - (2) As part of the request, the Subcontractor must provide the USAID Contracting Officer through JSI USAID Advancing Nutrition Director of Finance and Operations or a designee a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this Subcontract. The Subcontractor must simultaneously notify the USAID Contracting Officer’s Representative (COR) and the Office of the Chief Information

Office through JSI.

- (e) The USAID Contracting Officer through JSI USAID Advancing Nutrition Director of Finance and Operations or a designee will provide written approval to the Subcontractor expressly specifying the information technology equipment, software, or services approved for purchase by the USAID COR and the Agency CIO through JSI. Additional clauses or special contract requirements may be applicable and will be incorporated by the USAID Contracting Officer through JSI USAID Advancing Nutrition Director of Finance and Operations or a designee through a modification to the subcontract.
- (f) Except as specified in the USAID Contracting Officer's written approval provided through JSI USAID Advancing Nutrition Director of Finance and Operations or a designee, the Government or JSI are not obligated to reimburse the Subcontractor for costs incurred in excess of the information technology equipment, software or services specified in the Schedule.
- (g) The Subcontractor shall insert the substance of this special contract requirement, including this paragraph (g), in all subcontracts.

10. PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEMS INCIDENT REPORTING (APRIL 2018)

- (a) Definitions. As used in this special contract requirement-

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"Sensitive Information" or "Sensitive But Unclassified" Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS- 46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers,

"Personally Identifiable Information (PU)", means information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number (SSN), biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The definition of PU is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PU can become PU whenever additional information is made publicly available - in any medium and from any source - that, when combined with other available information, could be used to identify an individual. PU examples include name, address, SSN, or other identifying number or code, telephone number, and e-mail address. PU can also consist of a combination of indirect data elements such as gender, race, birth date, geographic indicator (e.g., zip code), and other descriptors used to identify specific individuals. When defining **PU** for USAID purposes, the term "individual" refers to a citizen of the United States or an alien lawfully admitted for permanent residence.

"National Security Information" means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified or national security information is specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

"Information Security Incident" means 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.

"Spillage" means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited, (i.e., authorized) for the applicable

security level of the data or information.

"Privacy Incident" means a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices, involving the breach of Personally Identifiable Information (PII), whether in electronic or paper format.

- (b) This special contract requirement applies to the Subcontractor and all personnel providing support under this subcontract (hereafter referred to collectively as "Subcontractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Privacy Act Compliance

Subcontractors must comply with the Privacy Act of 1974 requirements in the design, development, or operation of any system of records on individuals (as defined in FAR) containing PII developed or operated for USAID or to accomplish a USAID function for a System of Records (SOR).

(d) IT Security and Privacy Training

- (1) All Subcontractor personnel must complete USAID-provided mandatory security and privacy training prior to gaining access to USAID information systems and annually thereafter.
 - (2) The USAID Rules of Behavior and all subsequent updates apply to and must be signed by each user prior to gaining access to USAID facilities and information systems, periodically at the request of USAID. USAID will provide access to the rules of behavior and provide notification as required.
 - (3) Security and privacy refresher training must be completed on an annual basis by all Subcontractor and its lower tier subcontractor personnel providing support under this subcontract. USAID will provide notification and instructions on completing this training.
 - (4) Subcontractor employees filling roles identified by USAID as having significant security responsibilities must complete role-based training upon assignment of duties and thereafter at a minimum of every three years.
 - (5) Within fifteen (15) calendar days of completing the initial IT security training, the Subcontractor through JSI must notify the USAID COR in writing that its employees, in performance of the subcontract, have completed the training. The COR will inform the Subcontractor through JSI of any other training requirements.

(e) Information Security and Privacy Incidents

- (1) Information Security Incident Reporting Requirements: All Information Security Incidents involving USAID data or systems must be reported in accordance with the requirements below, even if it is believed that the incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.
 - (i) Subcontractor employees must report by e-mail all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer and Contracting Officer's Representative and the Contractor Facilities Security Officer. Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Subcontractor's discovery of a spillage or security incident involving classified information, the Subcontractor must immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or security incident in compliance with agency-specific instructions. The Subcontractor will abide by USAID instructions on correcting such a spill or security incident.

Subcontractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail concerning information security incident reports. To transmit Sensitive Information, Subcontractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.

(ii) The Subcontractor must provide any supplementary information or reports related to a previously reported incident directly to CIO-HELPDESK@usaid.gov, upon request. Correspondence must include related ticket number(s) as provided by the USAID Service Desk with the subject line "Action Required: Potential Security Incident".

(2) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information (PII), and can result in the loss of the public's trust and confidence in the Agency's ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. Subcontractor employees must report (by e-mail) all Privacy Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the incident, at: CIO-HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic). The subject line shall read "Action Required: Potential Privacy Incident".

(3) Information Security Incident Response Requirements

(i) All determinations related to Information Security and Privacy Incidents, associated with Information Systems or Information maintained by the Subcontractor in support of the activities authorized under this subcontract, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by USAID officials (except reporting criminal activity to law enforcement). The Subcontractor must not conduct any internal information security incident-related review or response activities that could modify or eliminate any existing technical configuration or information or forensic technical evidence existing at the time of the information security incident without approval from the Agency CIO communicated through the CO or COR.

(ii) The Subcontractor and Subcontractor employees must provide full and immediate access and cooperation for all activities USAID requests to facilitate Incident Response, including providing all requested images, log files, and event information to address and resolve Information Security Incidents.

(iii) Incident Response activities that USAID requires may include but are not limited to, inspections; investigations; forensic reviews; data analyses and processing.

(iv) At its discretion, USAID may obtain the assistance of Federal agencies and/or third party firms to aid in Incident Response activities.

(v) All determinations related to an Information Security Incident associated with Information Systems or Information maintained by the Subcontractor in support of the activities authorized by this subcontract will be made only by the USAID CIO through the CO or COR.

(vi) The Subcontractor must report criminal activity to law enforcement organizations upon becoming aware of such activity.

(f) The Subcontractor shall immediately notify the Contracting Officer in writing through JSI whenever it has reason to believe that the terms and conditions of the subcontract may be affected as a result of the reported incident.

The Subcontractor is required to include the substance of this provision in all subcontracts. In altering this special contract requirement, require subcontractors to report (by e-mail) information security and privacy incidents directly to the USAID Service Desk at CIO-HELPDESK@usaid.gov. A copy of the correspondence shall be sent to the prime Contractor (or higher tier subcontractor) and the Contracting Officer referencing the ticket number provided by the CIO-HELPDESK.

11. SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APRIL 2018)

(a) Definitions. As used in this special contract requirement-

"Audit Review" means the audit and assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities and methods for mitigating them and assist in implementation of new security controls where required. These reviews are conducted periodically but at least annually, and may be performed by USAID Bureau for Management, Office of the Chief Information Officer (M/CIO) or designated independent assessors/auditors, USAID Office of Inspector General (OIG) as well as external governing bodies such as the Government Accountability Office (GAO).

"Authorizing Official" means a senior government official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and/or the Nation.

"Information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"Sensitive Information" or "Sensitive But Unclassified (SBU)" - Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS- 46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. "National Security Information" means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified or national security information is specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

"Information Technology Resources" means agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants to third parties which establish or support information technology not operated directly by the Federal Government. (OMB M-15-14)

(b) Applicability: This special contract requirement applies to the Subcontractor, its subcontractors, and all personnel providing support under this subcontract (hereafter referred to collectively as "Subcontractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E- Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Compliance with IT Security and Privacy Policies: The Subcontractor shall be responsible for implementing information security for all information systems procured, developed, deployed, and/or operated on behalf of the US Government. All Subcontractor personnel performing under this subcontract and Subcontractor equipment used to process or store USAID data, or to connect to USAID networks, must comply with Agency information security requirements as well as current Federal regulations and guidance found in the Federal Information Security Modernization Act (FISMA), Privacy Act of 1974, E-Government Act of 2002, Section 208, and National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and

other relevant Federal laws and regulations that are applicable to USAID. The Subcontractor must comply with the following:

(1) HSPD-12 Compliance

- (i) Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.
- (ii) All development for USAID systems must include requirements to enable the use Personal Identity Verification (PIV) credentials, in accordance with NIST PIPS 201, PIV of Federal Employees and Contractors, prior to being operational or updated.

(2) Internet Protocol Version 6 (IPv6) or current version: This acquisition requires all functionality, capabilities and features to be supported and operational in both a dual-stack IPv4/IPv6 environment and an IPv6 only environment. Furthermore, all management, user interfaces, configuration options, reports and other administrative capabilities that support IPv4 functionality will support comparable IPv6 functionality. The Subcontractor is required to certify that its products have been tested to meet the requirements for both a dual-stack IPv4/IPv6 and IPv6-only environment. USAID reserves the right to require the Subcontractor's products to be tested within a USAID or third party test facility to show compliance with this requirement.

(3) Secure Configurations

- (i) The Subcontractor's applications must meet all functional requirements and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB) or the current configuration baseline.
- (ii) The standard installation, operation, maintenance, updates, and/or patching of software must not alter the configuration settings from the approved USGCB configuration. The information technology, when applicable, must also use the Windows Installer Service for installation to the default "program files" directory and must be able to silently install and uninstall.
- (iii) Applications designed for normal end users must run in the standard user context without elevated system administration privileges.
- (iv) The Subcontractor must apply due diligence at all times to ensure that the required level of security is always in place to protect USAID systems and information, such as using Defense Information Systems Agency Security Technical Implementation Guides (STIGs), common security configurations available from the National Institute of Standards and Technology's website at <https://nvd.nist.gov/ncp/repository> or USAID established configuration settings.

(4) PIPS 140 Encryption Requirements: Cryptographic modules used to protect USAID information must be compliant with the current PIPS 140 version and validated by the Cryptographic Module Validation Program (CMVP). The Subcontractor must provide the validation certificate number to USAID for verification. The Subcontractor is required to follow government-wide (PIPS 140) encryption standards.

(5) Security Monitoring, Auditing and Alerting Requirements: All Subcontractor-owned and operated systems that use or store USAID information must meet or exceed standards documented in this subcontract and in Service Level Agreements and Memorandums of Understanding/Agreements pertaining to security monitoring and alerting. These requirements include but are not limited to:

System and Network Visibility and Policy Enforcement at the following levels:

- Edge
- Server/ Host
- Workstation / Laptop / Client
- Network
- Application
- Database
- Storage
- User
- Alerting and Monitoring

- System, User, and Data Segmentation

(6) Subcontractor System Oversight/Compliance

- (i) The federal government has the authority to conduct site reviews for compliance validation. Full cooperation by the Subcontractor is required for audits and forensic analysis.
- (ii) The Subcontractors must afford USAID the level of physical or logical access to the Subcontractor's facilities, installations, technical capabilities, operations, documentation, records, and databases to the extent required to support its security and privacy programs. This includes monitoring, inspection, investigation and audits to safeguard against threats and hazards to the integrity, availability and confidentiality of USAID data or information systems operated on behalf of USAID; and to preserve or retrieve evidence in the case of computer crimes.
- (iii) All Subcontractor systems must comply with Information Security Continuous Monitoring (ISCM) and Reporting as defined in a continuous monitoring plan, to include, but not limited to, both automated authenticated and unauthenticated scans of networks, operating systems, applications, and databases. The Subcontractor must provide a continuous monitoring plan in accordance with NIST standards, as well as scan results upon request or at a minimum monthly to the Contracting Officer Representative (COR) and Contracting Officer, in addition to the CIO at ITAuthorization@usaid.gov, copying the USAID Advancing Nutrition Project Director. Alternatively, the Subcontractor may allow USAID information security staff to run scans directly.
- (iv) The Subcontractors must comply with systems development and lifecycle management best practices and processes as defined by Bureau for Management, Office of The Chief Information Officer (M/CIO) USAID IT Project Governance standards and processes for approval of IT projects, for the acceptance of IT project deliverables, and for the project's progression through its life cycle.

(7) Security Assessment and Authorization (SA&A)

- (i) For all information systems procured, developed, deployed, and/or operated on behalf of the US Government information by the provision of this subcontract, the Subcontractor must provide a system security assessment and authorization work plan, including project management information, to demonstrate that it complies or will comply with the FISMA and NIST requirements. The work plan must be approved by the COR through JSI, in consultation with the USAID M/CIO Information Assurance Division.
- (ii) Prior to deployment of all information systems that transmit, store or process Government information, the Subcontractor must obtain through JSI an Authority to Operate (ATO) signed by a USAID Authorizing Official from the Contracting Officer or COR. The Subcontractor must adhere to current NIST guidance for SA&A activities and continuous monitoring activities thereafter.
- (iii) Prior to the SA&A, a Privacy Threshold Analysis (PTA) must be completed using the USAID Privacy Threshold Analysis Template. The completed PTA must be provided through JSI to the USAID Privacy Officer or designate to determine if a Privacy Impact Analysis (PIA) is required. If a determination is made that a PIA is required, it must be completed in accordance with the USAID PIA Template, which USAID will provide to the Subcontractor through JSI as necessary. All privacy requirements must be completed in coordination with the COR or other designated Government staff.
- (iv) Prior to the Agency security assessment, authorization and approval, the Subcontractor must coordinate with the COR and other Government personnel as required to complete the FIPS 199 Security categorization and to document the systems security control baseline.
- (v) All documentation must be prepared, stored, and managed in accordance with standards, templates and guidelines established by USAID M/CIO. The USAID M/CIO or designee must approve all SA&A requirements.
- (vi) In information systems owned or operated by a Subcontractor on behalf of an agency, or for information collected or maintained by or on behalf of the agency, an SA&A must be done independent of USAID, to include the selection of a Federal Risk and Authorization Management Program (FEDRAMP)

approved independent Third Party Assessor (3PAO). See approved list of Assessors at <https://www.fedramp.gov/>. The Subcontractor must submit a signed SA&A package approved by the 3PAO to USAID at saacapackages@usaid.gov at least sixty (60) calendar days prior to obtain the ATO for the IT system.

- (vii) USAID retains the right to deny or rescind the ATO for any system if it believes the package or system fails to meet the USAID security requirements. Moreover, USAID may or may not provide general or detailed guidance to the Subcontractor to improve the SA&A package or the overall security posture of the information system and may or may not require re-submission of the package upon completion of the modifications. USAID reserves the right to limit the number of resubmissions at its convenience and may determine a system's compliance to be insufficient at which time a final determination will be made to authorize or deny operation. USAID is the final authority on the compliance.
- (viii) The Subcontractor through JSI must submit SA&A packages to the CIO at least sixty (60) days prior to production or the expiration of the current ATO. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT)
- (ix) Once the USAID Chief Information Security Officer or designee determines the risks, the Subcontractor must ensure that all Plan of Action and Milestones resulting from security assessments and continuous monitoring are remediated within a time frame commensurate with the level of risk as follows:
- High Risk= 30 calendar days;
 - Moderate Risk= 60 calendar days; and
 - Low Risk = 180 calendar days.
- (8) Federal Reporting Requirements: Contractors and Subcontractors operating information systems on behalf of USAID must comply with FISMA reporting requirements. Monthly, quarterly and annual data collections will be coordinated by USAID. Data collections include but are not limited to, data feeds in a format consistent with Office of Management and Budget (OMB) requirements. The Subcontractor must provide timely responses through JSI as requested by USAID and OMB.
- (d) The Subcontractor shall include the substance of this special contract requirement, including this paragraph (d), in all subcontracts, including subcontracts for commercial items.