REQUEST FOR PROPOSAL

RFP No. FAST-2022-001

SUBCONTRACT:	Behavioral Economics Pilot Training Course
TYPE OF SUBCONTRACT:	Firm Fixed Price
PROJECT:	Fiscal Accountability and Sustainable Trade (FAST)
SUPERVISOR(s):	FAST COP or designate
PLACE OF PERFORMANCE:	Virtual Platform
RFP PUBLISHED:	April 8, 2022 6PM Eastern Standard Time (EST)
NOTIFICATION OF INTEREST AND QUESTIONS DUE BY:	April 15, 2022 6PM Eastern Standard Time (EST)
QUESTIONS RESPOND DUE BY:	April 22, 2022 6PM Eastern Standard Time (EST)
FINAL SUBMISSION OF PROPOSAL DUE BY:	April 29, 2022 6PM Eastern Standard Time (EST)
TENTATIVE START DATE:	May 23, 2022
COMPLETION DATE:	The course must be delivered by August 31, 2022. The final report will be delivered 2 weeks after the conclusion of the course.

DevTech Systems, Inc. (DevTech) is an international consulting firm dedicated to development, with over 30 years of experience providing advisory services and technical assistance to government, private sector, and civil society stakeholders in more than 100 countries. We are a data driven organization that specializes in informing policy making by delivering focused data-driven evidence-based analysis products and services. DevTech core practice areas include Economic and Data analysis, Monitoring and Evaluation, Education and Youth Development, Gender and Inclusive Development, and Public Financial Management.

The Fiscal Accountability and Sustainable Trade (FAST) task order supports rapid, sustainable, and equitable economic growth in USAID-assisted countries by enabling the Agency to bring a systems approach to addressing Public Financial Management (PFM; public revenue, budget, expenditure, and debt), trade capacity building (TCB), macroeconomic planning and policies, and other economic governance issues, such as regulatory reform, and by supporting Missions to improve 1) host-country capacity to mobilize revenue and provide public services; 2) the policy climate for investment that generates more productive employment and inclusive growth, including issues specific to women and disadvantaged populations; 3) the host-country's ability to recover from, prevent, and/or mitigate the impact of conflict, natural disasters, or fiscal crises; and 4) the host-country's institutional capacity to identify, design, advocate, and implement better economic policies to enhance inclusive growth and gender equity.

Please submit your most competitive proposals in accordance with the instructions to offers and terms of reference. Any award issued as a result of this RFP will be subject to all instructions, terms of reference/specifications, certifications, terms and conditions, and funder required clauses.

1. BACKGROUND

Effective sustainable development policies and interventions require an understanding of how people think, and how society and history form behavior. Cognitive biases, decision heuristics, and social norms impact how a USAID-supported project is implemented and its desired outcomes. While the applicability of behavioral economics in development has been highlighted in recent years, the inclusion of behavioral economics in USAID programming has been limited.[1] The use of behavioral economics in USAID initiatives has been restricted primarily to global health reforms, such as Water Sanitation and Hygiene (WASH).

In alignment with USAID Administrator Samantha Power's proposed push to leverage behavioral economics to improve development programming, the DDI's Center for Economics and Market Development (EMD) has determined there is both great need and deep interest in providing technical training of USAID staff in behavioral economics and its application to development programming. To meet this need, EMD proposes the creation of a course structured as a primer on behavioral economics and its application to development challenges. This course will be a jumping off-point for expanding its use.

Definition of Behavioral Economics

For this course, the definition of behavioral economics that will be used is consistent with Kremer et al.'s definition in the *Handbook of Behavioral Economics*, Chapter 5, (2019) pg. 347:

[1] See the World Bank's 2015 World Development Report and in Kremer et al.'s (2019) Chapter 5 in *the Handbook of Behavioral Economics*

"We view behavioral economics as consisting of systematic deviations from the standard economic model in terms of preferences, beliefs, and decision-making. These deviations are motivated by insights from psychology but are typically captured using economic models. ... we extend this definition to include systematic deviations by firms from profit-maximization, even if the underlying psychology is not yet well understood."

2. SCOPE OF WORK

Objectives

The creation of a pilot training course on behavioral economics in development in both theory and practice.

The purpose of this project is three-fold:

1. Provide a primer in behavioral science and economics to USAID staff, in the form of a training course, covering biases, decision theory, mental models, and how they can both hinder and be leveraged by economic growth and related programming.
2. Create a pilot training course to evaluate what methods of instruction are best suited for participants and the themes and subtopics that would be most useful for USAID programming.
3. Create and foster a community of USAID trained staff that have the knowledge and skills to promote behavioral and experimental economics insights within their Missions, Bureaus, and Operating Units. This community will champion the inclusion of behavioral economics and science in the Agency.

This course will be an introduction to behavioral economics for participants and will abide closely by the definition of behavioral economics provided above. Additionally, the course will cover five themes. The course will cover the implementation of behavioral economics across USAID programming including health, anti-corruption, gender equality, education, public financial management, democracy, and human rights.

Additionally, while the concepts and themes in this course are applicable to all regions and all USAID partner countries, the cases and examples chosen from the field should be focused on developing countries, particularly on West Africa.

Tasks

The vendor will

A. Prepare a **workplan with a curriculum outline** (15-20 pages), which must present the chosen approach, method of instruction, and plan for all tasks under this contract. At a minimum, the workplan must:
    a. Describe the chosen topics and subtopics. They must fall under the five key themes.

b. List the experts and development practitioners that will present and facilitate the course
c. List the break-out room facilitators
d. Propose the prospective schedule, including days and times of the sessions
e. Propose the virtual platform to deliver this course

B. Design, organize, and conduct a **seven-day course, for four hours a day, on behavioral science and economics in development**. Each day will consist of lectures, break-out sessions (where participants will work collaboratively), and individual work. The organization of this course must include:
    a. Design of a schedule, which includes dates and times of lectures and break-out rooms and the descriptions of the lectures, and the topics covered
    b. Use of a trustworthy access platform on which to provide the course
    c. IT support for lecturers and participants
    d. The provision of course resources, prior to and during the course
    e. Communication to participants prior to and during the course (this includes relaying initial information but also reminder notifications throughout)
    f. Registration of participants prior to the course to correctly separate them into groups according to their interests and work
C. Create **pre-and post-surveys** for participants to gauge their comprehension of the material (the post survey will also include questions regarding the participants' opinions on the course structure and content).
D. Provide a **final report** (5-10 pages) on the implementation of the pilot course. The report will cover:
    a. A description of the course, including the topics included, the lecturers, and development practitioners who facilitated
    b. Discussion of the successes of the course, as well as the areas that require modifications
    c. The results of the surveys conducted before and after the course
    d. Final course materials, in digital format, including presenter and lecturer facilitator notes and breakout room guidelines
    e. Suggestions on how to improve the course for future iterations

Key Themes

The course must cover five key themes.

The themes are:

1. **Cognitive Biases:** The *homo economicus*, as presented in traditional economics, is rational, utility-maximizing, and self-interested, and is also equipped with perfect information. However, in reality, most individuals have biases which, even with perfect information, may make them act in ways that go against their self-interest or actually lower their utility. Within the field of development, notable biases include risk aversion, present bias, and confirmation bias.

2. **Decision Theory and Framing:** Individuals do not always process information or make decisions in a rational manner. The context of a decision and the available options impacts the choice an individual makes. This theme includes decision heuristics (anchoring, availability, and anchoring and adjustment heuristics), information overloading, risk perception, and framing the manner in which options and questions are presented and seen by the individual.

Themes one and two also include the introduction and use of nudges and choice architecture, both theoretically and in practice. These two interventions could be used in a multitude of areas, including taxation compliance, voting, public information campaigns, and public health measures.

3. **Impact of Poverty, Conflict, and Fragility on Decision Theory and Biases:** Long-term instability, whether due to poverty, violence, or poor governance, can lead to long-held beliefs and attitudes towards an individual's group, other societal groups, and the government. Individuals who have lived through a conflict may have discriminatory beliefs against those outside of their own group. Citizens in countries that have experienced long-term fragility may be hesitant to trust any form of government. Poverty impedes the ability of individuals with thoughts of scarcity.
4. **Mental Models:** Individuals do not make decisions or form preferences in a vacuum; they are socialized into holding specific worldviews, beliefs, and habits which impact the decisions they make and the social norms that they choose to uphold. These socially created mental models affect behavior and social change. Mental models impact how individuals, groups, and communities view gender, corruption, societal trust, and other ethnic/religious groups.
5. **Improving Programmatic Approaches in Development:** Development practitioners, donors, multilateral, and bilateral, and other international institutions are also susceptible to biases, social influences, and cognitive limitations. These impact their ability to design and implement projects that are sustainable and effective. The course will give USAID staff a framework to understand the lives and decisions of the poor. Biases also affect donors' decisions made during research and project implementation. The sunk cost of a project may influence a practitioner's decision on proceeding or ending a project. Social and cultural norms, as well as confirmation bias, affect how data and research are interpreted.

Proposals are also welcomed to include additional topics as long they are applicable to the field of development.

The course should allow opportunity for external speakers, provided by USAID.

Within these themes, there are many subtopics that can be used to solidify the material and to show the applicability and versatility of behavioral economics in development. Examples of subtopics include technology adoption, savings and insurance use, and workplace incentives.

Each theme will cover both theory and practice, prioritizing work done in developing countries. While the theory component is important for introducing behavioral economics concepts to participants, its purpose is to provide a foundational understanding for practically implementing

behavioral economics in the field. The practical component will include presentations of field experience, examples of testing solutions and designs, project design and implementation exercises, and discussions of the obstacles and enablers of behavioral economics interventions.

The course can be based on pre-existing materials or lectures, provided the subcontractor has full authority to use the materials, and deliver to DevTech for unrestricted future use.

Course Structure

This course will be delivered over **7 working days, for four hours a day**. The course will include lecturers who are leading experts in the field and development practitioners. It will include break-out sessions of small groups and individual work.

The **lectures** can utilize different mediums for instruction, including but not limited to PowerPoint presentations, videos, debates, and exercises. The course must have a good balance of experts and development practitioners. The inclusion of **development practitioners** with first-hand experience is required. These practitioners will share the enablers and barriers of implementing behavioral economics interventions in the field.

The **break-out sessions** will be used to review and discuss the content from the lectures, evaluate the barriers and enablers of implementing behavioral economics in the development field, and how behavioral economics can support USAID's agenda. The break-out rooms will cover real development challenges that USAID staff could face and work collaboratively to apply the learnings from the lectures to find a solution using behavioral economics concepts. Facilitators of the break-out sessions should be prepared to present hypothetical cases related to USAID-programming if participants are unable to provide real cases. This exercise will include designing a testing method for interventions, learning how to read and understand testing results, designing a project that utilizes behavioral economics, and addressing issues that may arise.

Within the break-out sessions and lectures, participants will be able to discuss any relevant development challenges and attempt to apply behavioral economics concepts and strategies during exercises.

Through this course structure, the participants will cultivate a sense of community, where they can work collaboratively in the future on the inclusion of behavioral economics and science in projects and initiatives.

Logistics

Participants

The course will be delivered to **30 participants**. They will be from USAID headquarters in Washington, D.C., and USAID missions around the world. The participants work on a wide range of issues, from public health to governance to gender equality. The participants will be taking the course from locations on different continents.

Course Platform

The course will be delivered virtually using an accessible, consistent, and trustworthy platform, such as Google, Zoom, Skype, etc to be proposed and facilitated by the subcontractor.

3. ORGANIZATIONAL MINIMUM REQUIREMENTS

The organization should possess the following experience and qualifications

A. Legally registered entity, with DUNS and SAM registration, capable of receiving US Government funding
B. Able to provide evidence of responsibility that the organization can manage and deliver assignments of this scope
C. Signed Representations and Certifications (Annex B)

4. KEY PERSONNEL

The Offeror should provide as a minimum the following key personnel with the following qualifications:

A. Team coordinator. This individual is responsible for providing consistent communication with the FAST team and for ensuring that the workplan and course are quality and are consistent with FAST standards. Their qualifications must include:
    a. Minimum Master's degree in economics, psychology, behavioral science, management, business, or development
    b. 5+ years' experience on research projects and training operations
    c. Experience coordinating and delivering training materials and sessions consistent with educational best practices
    d. Knowledge of and experience discussing current USAID programming and frameworks
    e. Must have excellent communication and organizational skills
B. Chief/Lead Behavioral Economist. This individual is responsible for creating the curriculum outline; finalizing the experts, development practitioners, and breakout room facilitators; finalizing the topics and subtopics; and creating the overall structure and flow of the course. Their qualifications must include:
    a. Minimum graduate degree in economics, psychology, behavioral economics or related field
    b. 5+ years of combined experience in teaching, researching or implementing projects using behavioral economics
    c. Experience applying behavioral economics in developing countries

5. DELIVERABLES

To meet the requirements of the subcontract, the selected organization or vendor will develop and submit the following deliverables:

1. A detailed workplan with a draft curriculum outline. The work plan must be a comprehensive document (15-20 pages) including the approach, method of instruction, and any other required activities under this contract. At a minimum, the outline must:
    - Propose the topics that will be covered.
    - Propose the experts and development practitioners that are expected to present and facilitate the course

- Propose the prospective days and times of the sessions
- Propose the virtual platform to deliver this course NB: USAID is standardized on Google Meet, but this is not a requirement.

2. The course materials. These materials should be comprehensive and detailed, and will be used for the creation of future iterations of the behavioral economics training course for USAID. These materials must include:
    - Finalized schedule. This includes the dates and times of each of the lectures and breakout rooms, the logic behind their sequencing, and the key lessons that participants will need to absorb. The schedule also must include full descriptions (4-5 sentences) of each lecture, breakout room, and exercise.
    - Topics and subtopics, for both lectures and breakout rooms. Each lecture, and the related breakout room, should focus on a particular topic, under the five themes. Each description of a topic and subtopic must include the underlying research and theory, examples of interventions using this topic, and the enablers and barriers for implementation.
    - List of confirmed experts, development practitioners, and breakout room facilitators (with their CVs). This list must include the specific topic that each individual will present and discuss. Regarding the lectures, there must be a balance of experts and development practitioners.
    - Notes on the course. These notes must include the approach the vendor used for this course, the most important information and tools that students will gain from their participation, the hypothetical case studies for the breakout rooms, project design steps for implementing behavioral economics interventions in the field, and additional resources that participants can use to address development challenges using specific behavioral economics concepts.
    - Preliminary presentation outlines. These outlines must include the main ideas from the lectures, the proposed activities to solidify the lesson, and examples of field implementation.
3. A 7-day long course, 4 hours per day on behavioral economics in development. The course will be an introduction to behavioral economics for 30 participants from USAID. At a minimum, the course must:
    - Cover the five themes: cognitive biases, decision theory and framing, mental models, the impact of poverty, fragility, and conflict on biases and decision-making, and improving programmatic approaches for development.
    - Go over both theory and practice, with special attention paid to voices from the field.
    - Provide strategies and cases that participants can draw from to support their current and future projects.
    - Include lectures, break-out room group work, and individual work.
    - Design and conduct pre- and post-course surveys for participants
    - Create a final report that will provide a description of the course, discuss areas of success and failure, discuss the results of the surveys, and provide recommendations for future iterations.

4. A **final report** (5-10 pages) on the implementation of the pilot course. At a minimum, the report must cover:
    - A description of the course, including the topics included, the lecturers, and development practitioners who facilitated
    - Highlights of the successes of the course as well as the areas that require modifications
    - The results of the surveys conducted at the start of and at the end of the course
    - Suggestions on how to improve the course for future iterations

3. PAYMENT SCHEDULE

This subcontract will be disbursed in two payments, according to the submission and approval of the following products:

Deliverable	Payment	Due Date
Comprehensive workplan with draft curriculum outline	10%	2 weeks following the full execution of this contract
All course materials	50%	30 days prior to course delivery
Seven-day pilot course on behavioral economics in development	20%	By August 31, 2022
Final report	20%	2 weeks following the conclusion of the course
Total	**100%**	

All deliverables must be approved by DevTech Systems, Inc. prior to payment.

4. PROPOSAL SUBMISSION REQUIREMENTS

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 on or before the due date and time indicated in page 1 to the emails in Section H. Submission Instructions. Proposals must be submitted by email only and with the subject line "RFP No: FAST-2022-001.

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 make reference 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:

7.1 Technical Proposal

The Technical proposal shall describe how the offeror intends to carry out the Scope of Work. 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.

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.

The Technical Proposal should include the following sections:

A. **Organization Overview** - Legal name; year of incorporation; number of employees; description of all services and products supplied.
B. **Narrative** outlining how the applicant will successfully complete activities and responsibilities outlined in the scope of work. (up to 10 pages)
C. **Capabilities and Past Performance** - Description of applicable organizational capabilities/experience and major accomplishments in conducting job similar in size and complexity outlined in this scope of work in the last 5 years. Information of similar jobs should include funding agency and cost (up to five pages)
D. **Staffing Plan** - Provide a proposed staffing plan for the completion of the tasks the outlined in the SOW: workplan with curriculum outline, pilot training course, surveys, and final report. For the pilot training course, this includes a proposed list of lecturers (development practitioners and experts) and breakout room facilitators.
E. **Curriculum Vitae** of proposed key personnel (up to two pages each)
F. **Contact information** of three recent clients for similar activities. Please provide name, email and phone contact information.

Proposal should be no longer than 20 pages, excluding CVs. The proposals can also include the CVs of potential instructors. These CVs will be excluded from the 20-page maximum.

7.2 Cost Proposal

The offeror should submit their most competitive and complete cost proposal. The cost proposal shall be submitted in a separate volume from the technical proposal. An Excel template for the budget can be found here. The cost proposal shall be submitted as a firm-fixed price proposal in USD currency. The cost proposal shall include the following:

A. Cover sheet with organization information, including name, address, email, phone, DUNS number, and contact person. Please note that your organization needs to have an active registration in sam.gov (https://www.sam.gov/SAM/) in order to receive a contract for this activity. Registration is FREE, but needs to be done in advance in order to be registered. You will need your company DUNS number, which can be requested for FREE at SAM Webform : Home (dnb.com).
B. Audited Financial Statements for the past three years.
C. Evidence of Responsibility (see Annex A)
D. Certification Regarding Debarment, Suspension, or Proposed Debarment (see Annex D)
E. Representations, Certifications, and Other Statements of Bidders (see Annex B)
F. Acknowledgement of Contract Clauses (see Annex C)
G. A budget in Excel with the Offeror's fixed price for each deliverable, each of which will be considered a fixed price budget for that specific segment of work. The price 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. The budget must be completed in the attached budget template (see Annex E). It should include three tabs 1) Fixed price 2) Summary 3) Detailed budget. Any assumptions can be included in tab 4. itemized, proposed budget including, at minimum: wages, travel and transportation, and other direct costs. Proposed budget will be structured in accordance to the payment schedule in Section 4 above. Applicants are to include all costs deemed necessary to execute this SOW in the application budget.

H. A detailed budget narrative in word or pdf that justifies the cost as appropriate and necessary for the successful completion of proposed activities and deliverables. The budget narrative should clearly describe the project and cost assumptions. 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.

5. SUBMISSION INSTRUCTIONS

Notification of interest, all questions and final proposal should be submitted by the dates established on page 1 to usaidfast@gmail.com. No late submissions will be accepted.

6. PROPOSAL EVALUATION CRITERIA

Proposals shall be submitted according to Proposal Submission instructions above. Technical Proposal will be evaluated separately from the Cost Proposal. Award will be made to Offeror that submits the best value for money which is demonstrated by offeror proposal in showing the most advantageous combination of cost, quality and effort to meet SOW requirements.

Proposals will be evaluated first to ensure that they meet all mandatory requirements and responsive. To be determined responsive, a proposal must include all documentation as listed in Proposal Submission Requirements section. Proposals that fail to meet these requirements will receive no further consideration. A non-responsive proposal to any element may be eliminated from consideration.

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

Evaluation factors are as follows:

No.	Criteria	Points
1	Narrative and Staffing Plan 1. Extent to which the offeror demonstrates an understanding of the Scope of Work 2. Degree to which the proposed training program meets the objectives and purpose of the SOW.	50

	3. The stated willingness of the offeror to collaborate in a flexible way to work with DevTech and USAID.	
2	Key Personnel Demonstrated capability and experience of the proposed team leader to fulfill the requirements in section 4.	10
3	Corporate Capabilities Corporate experience in having provided similar training programs covering similar topics.	20
4	Proposed cost	20
	Total	100

7. TERMS OF AWARD

This document is a request for proposals only, and in no way obligates DevTech Systems 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 DevTech 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 DevTech. DevTech may choose to award a sub-contract for part of the activities in the RFP.

8. 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.

9. PAYMENT TERMS

DevTech 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 DevTech in meeting the terms and conditions of payment will be given the highest consideration.

10. 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. DevTech 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.

11. AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this award is "937".

Local procurements are to be accomplished in accordance with AIDAR 752.225-71 and ADS 311. Geographic Code 937 is defined as the United States, the cooperating country and developing countries other than advanced developing countries and excluding prohibited sources.

12. 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 sub-contract. The Project also reserves the right to conduct negotiations on technical, management, or cost issues prior to the award of a sub-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 sub-contract without any obligation to previously considered offerors.

13. REJECTION OF PROPOSALS

DevTech reserves the right to reject any and all proposals received, or to negotiate separately with any and all competing offerors, without explanation.

14. INCURRING COSTS

DevTech 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.

15. MODIFICATIONS

DevTech 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 RFP.

16. CANCELLATION

DevTech may cancel this RFP without any cost or obligation at any time until issuance of the award.

17. USAID REGULATIONS

The entity will ensure that all work activities conducted under this contract towards the successful completion of this scope of work is completed in accordance with all applicable USAID and USG regulations, including but not limited to 22 CFR, CFR 200, FAR and AIDAR.

ANNEX A

Evidence of Subcontractor/Subrecipient Responsibility Statement

1. Authorized Negotiators

(Company Name) proposal for (Proposal Name) may be discussed with any of the following individuals. These individuals are authorized to represent (Company Name) in negotiation of this offer.

(List Names of Authorized signatories)

These individuals can be reached at (Company Name) office:

Address
Telephone
Email

2. Adequate Financial Resources

(Company Name) has adequate financial resources to manage this subcontract, as established by our audited financial statements submitted in this proposal.

3. Ability to Comply

(Company Name) is able to comply with the proposed delivery of performance schedule having taken into consideration all existing business commitments, commercial as well as governmental.

4. Record of Performance, Integrity, and Business Ethics

Subcontractor/Subrecipient should insert a statement describing how long they have been in business, the types of contracts/agreements they have completed, etc. This section can also include a brief summary of internal controls and ethics policies.

5. Organization, Experience, Accounting and Operational Controls, and Technical Skills

(Subcontractor/Subrecipient should explain which department and/or technical practice group within the company will be managing the Subagreement. Please also include information on the type of accounting and control procedures the Subrecipient has to accommodate a Cost

Reimbursement type Subagreement)

6. Equipment and Facilities

(Subcontractor/Subrecipient should state if they have necessary facilities and equipment to carry out the subagreement)

7. Eligibility to Receive Award

(Subcontractor/Subrecipient should state if it is qualified and eligible to receive an award under applicable laws and regulation and if they have performed work of similar nature under similar mechanisms for USAID, any other federal agency, and/or international donor. The subrecipient should provide its DUNS number here as well.)

8. Cognizant Government Audit Agency

(Subcontractor/Subrecipient should provide Name, address, phone of their auditors – whether it is Defense Contractor Audit Agency (DCAA) or independent CPA if applicable.)

9. Recovery of Vacation, Holiday and Sick Pay

(Subcontractor/Subrecipient should explain how its recovers vacation, holiday, and sick leave)

Date:_____

Name:_____

Title: _____

Authorized Signature:_____

ANNEX B

SECTION K - Representations, Certifications, and Other Statements of Bidders

K.1 NOTICE LISTING SOLICITATION PROVISIONS INCORPORATED BYREFERENCE

The following contract clauses pertinent to this section are hereby incorporated by reference (byCitation Number, Title, and Date) in accordance with the clause at FAR 52.252-2 "CLAUSES INCORPORATED BY REFERENCE" in Section I of this contract. See http://acquisition.gov/far/index.html for electronic access to the full text of a FAR clause.

Number	Title	Date
Federal Acquisition Regulation (48 Cfr Chapter 1)		
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	(Sep 2007)
52.204-17	Ownership or Control of Offeror	(Jul 2016)
52.204-19	Incorporation by Reference Of Representations and Certifications	(Dec 2014)
52.209-2	Prohibition on Contracting With Inverted Domestic Corporations--Representation	(Nov 2015)
52.222-38	Compliance With Veterans' Employment Reporting Requirements	(Feb 2016)
52.225-25	Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating To Iran-Representation and Certifications	(Oct 2015)

K.2 52.204-8 ANNUAL RESPRESENTATIONS AND CERTIFICATIONS (JAN 2017)

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is _____ [insert NAICS code].

(2) The small business size standard is _____ [insert size standard].

(3) The small business size standard for a concern which submits an offer in its own name,

other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)(1) If the provision at 52.204-7, System for Award Management, is included in this solicitation, paragraph (d) of this provision applies.

(2) If the provision at 52.204-7 is not included in this solicitation, and 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 (d) 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 (d) applies.

☐ (ii) Paragraph (d) does not apply and the offeror has completed the individual representations and certifications in the solicitation.

(c)(1) The following representations or certifications in SAM are applicable to this solicitation as indicated:

(i) 52.203-2, Certificate of Independent Price Determination. This provision applies to solicitations when a firm-fixed-price contract or fixed-price contract with economic price adjustment is contemplated, unless—

(A) The acquisition is to be made under the simplified acquisition procedures in Part 13;

(B) The solicitation is a request for technical proposals under two-step sealed bidding procedures; or

(C) The solicitation is for utility services for which rates are set by law or regulation.

(ii) 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions. This provision applies to solicitations expected to exceed $150,000.

(iii) 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation. This provision applies to all solicitations.

(iv) 52.204-3, Taxpayer Identification. This provision applies to solicitations that do not include the provision at 52.204-7, System for Award Management.

(v) 52.204-5, Women-Owned Business (Other Than Small Business). This provision applies to solicitations that—

(A) Are not set aside for small business concerns;

(B) Exceed the simplified acquisition threshold; and

(C) Are for contracts that will be performed in the United States or its outlying areas.

(vi) 52.209-2, Prohibition on Contracting with Inverted Domestic Corporations—Representation.

(vii) 52.209-5, Certification Regarding Responsibility Matters. This provision applies to solicitations where the contract value is expected to exceed the simplified acquisition threshold.

(viii) 52.209-11, Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law. This provision applies to all solicitations.

(ix) 52.214-14, Place of Performance—Sealed Bidding. This provision applies to invitations for bids except those in which the place of performance is specified by the Government.
(x) 52.215-6, Place of Performance. This provision applies to solicitations unless the place of performance is specified by the Government.
(xi) 52.219-1, Small Business Program Representations (Basic & Alternate I). This provision applies to solicitations when the contract will be performed in the United States or its outlying areas.

(A) The basic provision applies when the solicitations are issued by other than DoD, NASA, and the Coast Guard.
(B) The provision with its Alternate I applies to solicitations issued by DoD, NASA, or the Coast Guard.

(xii) 52.219-2, Equal Low Bids. This provision applies to solicitations when contracting by sealed bidding and the contract will be performed in the United States or its outlying areas.
(xiii) 52.222-22, Previous Contracts and Compliance Reports. This provision applies to solicitations that include the clause at 52.222-26, Equal Opportunity.
(xiv) 52.222-25, Affirmative Action Compliance. This provision applies to solicitations, other than those for construction, when the solicitation includes the clause at 52.222-26, Equal Opportunity.
(xv) 52.222-38, Compliance with Veterans' Employment Reporting Requirements. This provision applies to solicitations when it is anticipated the contract award will exceed the simplified acquisition threshold and the contract is not for acquisition of commercial items.
(xvi) 52.222-57, Representation Regarding Compliance with Labor Laws (Executive Order 13673). This provision applies to solicitations expected to exceed $50 million which are issued from October 25, 2016 through April 24, 2017, and solicitations expected to exceed $500,000, which are issued after April 24, 2017.
Note to paragraph (c)(1)(xvi): By a court order issued on October 24, 2016, 52.222-57 is enjoined indefinitely as of the date of the order. The enjoined paragraph will become effective immediately if the court terminates the injunction. At that time, GSA, DoD and NASA will publish a document in the Federal Register advising the public of the termination of the injunction.
(xvii) 52.223-1, Biobased Product Certification. This provision applies to solicitations that require the delivery or specify the use of USDA–designated items; or include the clause at 52.223-2, Affirmative Procurement of Biobased Products Under Service and Construction Contracts.
(xviii) 52.223-4, Recovered Material Certification. This provision applies to solicitations that are for, or specify the use of, EPA–designated items.
(xix) 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals–Representation. This provision applies to solicitation that include the clause at 52.204-7.
(xx) 52.225-2, Buy American Certificate. This provision applies to solicitations containing the clause at 52.225-1.
(xxi) 52.225-4, Buy American—Free Trade Agreements—Israeli Trade Act Certificate. (Basic, Alternates I, II, and III.) This provision applies to solicitations containing the clause at 52.225-3.

(A) If the acquisition value is less than $25,000, the basic provision applies.
(B) If the acquisition value is $25,000 or more but is less than $50,000, the provision with its Alternate I applies.
(C) If the acquisition value is $50,000 or more but is less than $77,533, the provision with its Alternate II applies.
(D) If the acquisition value is $77,533 or more but is less than $100,000, the provision with its Alternate III applies.

(xxii) 52.225-6, Trade Agreements Certificate. This provision applies to solicitations containing the clause at 52.225-5.
(xxiii) 52.225-20, Prohibition on Conducting Restricted Business Operations in Sudan—Certification. This provision applies to all solicitations.
(xxiv) 52.225-25, Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran-Representation and Certifications. This provision applies to all solicitations.
(xxv) 52.226-2, Historically Black College or University and Minority Institution Representation. This provision applies to solicitations for research, studies, supplies, or services of the type normally acquired from higher educational institutions.

(2) The following representations or certifications are applicable as indicated by the Contracting Officer:
[Contracting Officer check as appropriate.]
__ (i) 52.204-17, Ownership or Control of Offeror.
__ (ii) 52.204-20, Predecessor of Offeror.
__ (iii) 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products.
__ (iv) 52.222-48, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment- Certification.
__ (v) 52.222-52, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Certification.
__ (vi) 52.223-9, with its Alternate I, Estimate of Percentage of Recovered Material Content for EPA–Designated Products (Alternate I only).
__ (vii) 52.227-6, Royalty Information.
__ (A) Basic.
__(B) Alternate I.
__ (viii) 52.227-15, Representation of Limited Rights Data and Restricted Computer Software.

(d) The offeror has completed the annual representations and certifications electronically via the SAM website 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 (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.
FAR CLAUSE # TITLE DATE CHANGE

_____ _____ _____ _____
Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on SAM.

K.3 52.204-20 PREDECESSOR OF OFFEROR (JUL 2016)

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

"Commercial and Government Entity (CAGE) code" means—

(1) An identifier assigned to entities located in the United States and its outlying areas by the Defense Logistics Agency (DLA) Contractor and Government Entity (CAGE) Branch to identify a commercial or government entity, or
(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of code is known as a NATO CAGE (NCAGE) code.

"Predecessor" means an entity that is replaced by a successor and includes any predecessors of the predecessor.

"Successor" means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

(b) The Offeror represents that it [ ] is or [ ] is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(c) If the Offeror has indicated "is" in paragraph (b) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: _____ (or mark "Unknown").

Predecessor legal name: _____.
(Do not use a "doing business as" name).

K.4 52.209-5 CERTIFICATION REGARDING RESPONSIBILITY MATTERS (OCT 2015)

(a)

(1) The Offeror certifies, to the best of its knowledge and belief, that --

(i) The Offeror and/or any of its Principals --

(A) Are [_] are not [_] presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(B) 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 public (Federal, State, or local) 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 (if offeror checks "have", the offeror shall alsosee 52.209-7, if included in this solicitation); and

(C) Are [_] are not [_] presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision; and
(D) 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.

(1) Federal taxes are considered delinquent if both of the following criteria apply:

(i) 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.

(ii) 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.

(2) Examples.

(i) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(ii) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(iii) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(iv) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. 362 (the Bankruptcy Code).

(ii) The Offeror has [[_] has not [_], within a three-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principal," for the purposes of this certification, means an officer; director; owner; partner; or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

This Certification Concerns a Matter Within the Jurisdiction of an Agency of the United States and the Making of a False, Fictitious, or Fraudulent Certification May Render the Maker Subject to Prosecution Under Section 1001, Title 18, United States Code.

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the certification will be considered in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a) of this provision. The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

K.5 52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (JUL 2013)

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

"Administrative proceeding" means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (*e.g.*, Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceeding at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

"Federal contracts and grants with total value greater than $10,000,000" means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

"Principal" means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [_] has [_] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management database via https://www.acquisition.gov (see 52.204-7).

K.6 52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (FEB 2016)

(a) 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--

(1) 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

(2) 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.

(b) The Offeror represents that—

(1) 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

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

K.7 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS

(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)
(1) The North American Industry Classification System (NAICS) code for this acquisition is 541990.
(2) The small business size standard is $15.0 million.
(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(c) *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 (c)(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 (c)(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 (c)(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 (c)(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 (c)(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 (c)(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 (c)(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 (c)(6) of this provision.*] The offeror represents as part of its offer that is [_] 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 (c)(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 (c)(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.

(d) *Notice*.

(1) If this solicitation is for supplies and has been set aside, in whole or in part, for small business concerns, then the clause in this solicitation providing notice of the set-aside contains restrictions on the source of the end items to be furnished.

(2) Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a business concern that is small, HUBZone small, small disadvantaged, service-disabled veteranowned small, economically disadvantaged women-owned small, or women-owned small eligible under the WOSB Program in order to obtain a contract to be awarded under the preference programs established pursuant to section 8, 9, 15, 31, and 36 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, shall –

(i) Be punished by imposition of fine, imprisonment, or both;

(ii) Be subject to administrative remedies, including suspension and debarment; and

(iii) Be ineligible for participation in programs conducted under the authority of the Act.

Alternate I (Sep 2015). As prescribed in **19.309**(a)(2), add the following paragraph (c)(9) to the basic provision:

(9) [Complete if offeror represented itself as disadvantaged in paragraph (c)(2) of this provision.] The offeror shall check the category in which its ownership falls:

___ Black American.
___ Hispanic American.
___ Native American (American Indians, Eskimos, Aleuts, or Native Hawaiians).
___ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, Republic of Palau, Republic of the Marshall Islands, Federated States of Micronesia, the Commonwealth of the Northern Mariana Islands, Guam, Samoa, Macao, Hong Kong, Fiji, Tonga, Kiribati, Tuvalu, or Nauru).
___ Subcontinent Asian (Asian-Indian) American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).
___ Individual/concern, other than one of the preceding.

K.8 52.222-22 PREVIOUS CONTRACTS AND COMPLIANCE REPORTS (FEB 1999)

The offeror represents that --

(a) It [_] has, [_] has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation;
(b) It [_] has, [_] has not filed all required compliance reports; and
(c) Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

K.9 52.222-25 AFFIRMATIVE ACTION COMPLIANCE (APR 1984)

The offeror represents that --

(a) It [_] has developed and has on file, [_] has not developed and does not have on file, at each establishment, affirmative action programs required by the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2); or
(b) It [_] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

K.10 52.225-20 Prohibition on Conducting Restricted Business Operations in Sudan—Certification (Aug 2009)

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

"Business operations" means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

"Marginalized populations of Sudan" means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and
(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

"Restricted business operations" means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;
(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization ;
(3) Consist of providing goods or services to marginalized populations of Sudan;
(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;
(5) Consist of providing goods or services that are used only to promote health or education; or
(6) Have been voluntarily suspend.

(b) *Certification*. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

K.11 52.230-1 COST ACCOUNTING STANDARDS NOTICES AND CERTIFICATION (OCT 2015)

Note: This notice does not apply to small businesses or foreign governments. This notice is in three parts, identified by Roman numerals I through III.

Offerors shall examine each part and provide the requested information in order to determine Cost Accounting Standards (CAS) requirements applicable to any resultant contract.

If the offeror is an educational institution, Part II does not apply unless the contemplated contract will be subject to full or modified CAS coverage pursuant to 48 CFR 9903.201-2(c)(5) or 9903.201-2(c)(6), respectively.

I. Disclosure Statement -- Cost Accounting Practices and Certification

(a) Any contract in excess of $750,000 resulting from this solicitation will be subject to the requirements of the Cost Accounting Standards Board (48 CFR Chapter 99), except for those contracts which are exempt as specified in 48 CFR 9903.201-1.
(b) Any offeror submitting a proposal which, if accepted, will result in a contract subject to the requirements of 48 CFR Chapter 99 must, as a condition of contracting, submit a Disclosure Statement as required by 48 CFR 9903.202. When required, the Disclosure Statement must be submitted as a part of the offeror's proposal under this solicitation unless the offeror has already submitted a Disclosure Statement disclosing the practices used in connection with the pricing of this proposal. If an applicable Disclosure Statement has already been submitted, the offeror may satisfy the requirement for submission by providing the information requested in paragraph (c) of Part I of this provision.

Caution: In the absence of specific regulations or agreement, a practice disclosed in a Disclosure Statement shall not, by virtue of such disclosure, be deemed to be a proper, approved, or agreed-to practice for pricing proposals or accumulating and reporting contract performance cost data.

(c) Check the appropriate box below:

[_] (1) *Certificate of Concurrent Submission of Disclosure Statement.* The offeror hereby certifies that, as a part of the offer, copies of the Disclosure Statement have been submitted as follows:

(i) Original and one copy to the cognizant Administrative Contracting Officer (ACO) or cognizant Federal agency official authorized to act in that capacity (Federal official), as applicable; and
(ii) One copy to the cognizant Federal auditor.

(Disclosure must be on Form No. CASB DS-1 or CASB DS-2, as applicable. Forms may be obtained from the cognizant ACO or Federal official and/or from the looseleaf version of the Federal Acquisition Regulation.)

Date of Disclosure Statement: _____
Name and Address of Cognizant ACO or Federal Official Where Filed:

_____

The offeror further certifies that the practices used in estimating costs in pricing this proposal are consistent with the cost accounting practices disclosed in the Disclosure Statement.

[_] (2) *Certificate of Previously Submitted Disclosure Statement.* The offeror hereby certifies that the required Disclosure Statement was filed as follows:

Date of Disclosure Statement: _____
Name and Address of Cognizant ACO or Federal Official Where Filed:

_____

The offeror further certifies that the practices used in estimating costs in pricing this proposal are consistent with the cost accounting practices disclosed in the applicable Disclosure Statement.

[_] (3) *Certificate of Monetary Exemption.* The offeror hereby certifies that the offeror, together with all divisions, subsidiaries, and affiliates under common control, did not receive net awards of negotiated prime contracts and subcontracts subject to CAS totaling $50 million or more in the cost accounting period immediately preceding the period in which this proposal was submitted. The offeror further certifies that if such status changes before an award resulting from this proposal, the offeror will advise the Contracting Officer immediately.

[_] (4) *Certificate of Interim Exemption.* The offeror hereby certifies that

(i) the offeror first exceeded the monetary exemption for disclosure, as defined in (3) of this subsection, in the cost accounting period immediately preceding the period in which this offer was submitted and

(ii) in accordance with 48 CFR 9903.202-1, the offeror is not yet required to submit a Disclosure Statement. The offeror further certifies that if an award resulting from this proposal has not been made within 90 days after the end of that period, the offeror will immediately submit a revised certificate to the Contracting Officer, in the form specified under subparagraph (c)(1) or (c)(2) of Part I of this provision, as appropriate, to verify submission of a completed Disclosure Statement.

Caution: Offerors currently required to disclose because they were awarded a CAS-covered prime contract or subcontract of $50 million or more in the current cost accounting period may not claim this exemption (4). Further, the exemption applies only in connection with proposals submitted before expiration of the 90-day period following the cost accounting period in which the monetary exemption was exceeded.

II. Cost Accounting Standards -- Eligibility for Modified Contract Coverage

If the offeror is eligible to use the modified provisions of 48 CFR 9903.201-2(b) and elects to do so, the offeror shall indicate by checking the box below. Checking the box below shall mean that the resultant contract is subject to the Disclosure and Consistency of Cost Accounting Practices clause in lieu of the Cost Accounting Standards clause.

[_] The offeror hereby claims an exemption from the Cost Accounting Standards clause under the provisions of 48 CFR 9903.201-2(b) and certifies that the offeror is eligible for use of the Disclosure and Consistency of Cost Accounting Practices clause because during the cost accounting period immediately preceding the period in which this proposal was submitted, the offeror received less than $50 million in awards of CAS-covered prime contracts and subcontracts. The offeror further certifies that if such status changes before an award resulting from this proposal, the offeror will advise the Contracting Officer immediately.

Caution: An offeror may not claim the above eligibility for modified contract coverage if this proposal is expected to result in the award of a CAS-covered contract of $50 million or more or if, during its current cost accounting period, the offeror has been awarded a single CAS-covered prime contract or subcontract of $50 million or more.

III. Additional Cost Accounting Standards Applicable to Existing Contracts

The offeror shall indicate below whether award of the contemplated contract would, in accordance with subparagraph (a)(3) of the Cost Accounting Standards clause, require a change in established cost accounting practices affecting existing contracts and subcontracts.
[_] yes [_] no

K.12 52.230-7 PROPOSAL DISCLOSURE – COST ACCOUNTING PRACTICE CHANGES (APR 2005)

The offeror shall check "yes" below if the contract award will result in a required or unilateral change in cost accounting practice, including unilateral changes requested to be desirable changes.

[ ] Yes [ ] No

If the offeror checked "Yes" above, the offeror shall--

(1) Prepare the price proposal in response to the solicitation using the changed practice for the period of performance for which the practice will be used; and

(2) Submit a description of the changed cost accounting practice to the Contracting Officer and the Cognizant Federal Agency Official as pricing support for the proposal.

Date of Offer:

Name of Offeror:

Typed Name and Title:

Signature_____Date:

ANNEX C

SECTION H and I – CONTRACT CLAUSES

H.23 RESTRICTIONS AGAINST DISCLOSURE (MAY 2016)

(a) The Contractor agrees, in the performance of this contract, to keep the information furnished by the Government or acquired/developed by the Contractor in performance of the contract and designated by the Contracting Officer or Contracting Officer's Representative, in the strictest confidence. The Contractor also agrees not to publish or otherwise divulge such information, in whole or in part, in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to restrict access to such information while in the Contractor's possession, to those employees needing such information to perform the work described herein, i.e., on a "need-to-know" basis. The Contractor agrees to immediately notify the Contracting Officer in writing in the event that the Contractor determines or has reason to suspect a breach of this requirement has occurred.

(b) All Contractor staff working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

(c) The Contractor shall insert the substance of this special contract requirement, including this paragraph (c), in all subcontracts when requiring a restriction on the release of information developed or obtained in connection with performance of the contract.

H.26 INFORMATION TECHNOLOGY APPROVAL (APRIL 2018) (DEVIATION NO. M/OAA-DEV-FAR-18-2C)

(a) Definitions. As used in this contract –

"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 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 contract. The Contractor must not acquire additional information technology without the prior written approval of the Contracting Officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor 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 Government's statement of work, the Contractor must request prior written approval from the Contracting Officer.
(2) As part of the request, the Contractor must provide the Contracting Officer a description and an estimate of the total cost of the information technology equipment, software, or services to be procured under this contract. The Contractor must simultaneously notify the Contracting Officer's Representative (COR) and the Office of the Chief Information Officer at **ITAuthorization@usaid.gov**.

(e) The Contracting Officer will provide written approval to the Contractor expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. Additional clauses or special contract requirements may be applicable and will be incorporated by the Contracting Officer through a modification to the contract.

(f) Except as specified in the Contracting Officer's written approval, the Government is not obligated to reimburse the Contractor for costs incurred in excess of the information technology equipment, software or services specified in the Schedule.

(g) The Contractor shall insert the substance of this special contract requirement, including this paragraph (g), in all subcontracts.

H.27 MEDIA AND INFORMATION HANDLING AND PROTECTION (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. This also includes but not limited to all records, files, and metadata in electronic or hardcopy format.
"Sensitive Information or Sensitive But Unclassified" (SBU) means 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;DS61;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

"Media" means physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

(b) This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") 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), EGovernment 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) Handling and Protection. The Contractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. The Contractor must develop and implement policies or documentation regarding the protection, handling, and destruction of Sensitive Information. The policy or procedure must address at a minimum, the requirements documented in NIST 800-53 Revision 4 or the current revision for Media Protection Controls as well as the following:

(1) Proper marking, control, storage and handling of Sensitive Information residing on electronic media, including computers and removable media, and on paper documents.
(2) Proper security, control, and storage of mobile technology, portable data storage devices, and communication devices.
(3) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information while at rest and in transit throughout USAID, contractor, and/or subcontractor networks, and on host and client platforms.
(4) Proper use of FIPS 140-2 compliant encryption methods to protect Sensitive Information in email attachments, including policy that passwords must not be communicated in the same email as the attachment.

(d) Return of all USAID Agency records. Within five (5) business days after the expiration or termination of the contract, the contractor must return all Agency records and media provided by USAID and/or obtained by the Contractor while conducting activities in accordance with the contract.

(e) Destruction of Sensitive Information: Within twenty (20) business days after USAID has received all Agency records and media, the Contractor must execute secure destruction (either by the contractor or third party firm approved in advance by USAID) of all remaining originals and/or copies of information or media provided by USAID and/or obtained by the Contractor while conducting activities in accordance with the contract. After the destruction of all information and media, the contractor must provide USAID with written confirmation verifying secure destruction.

(f) The Contractor shall include the substance of this special contract requirement in all subcontracts, including this paragraph (f).

H.28 PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEMS INCIDENT REPORTING (APRIL 2018)

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 (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.

"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.

1. This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") 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.

2. Privacy Act Compliance

Contractors 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).

3. IT Security and Privacy Training

a. All Contractor personnel must complete USAID-provided mandatory security and privacy training prior to gaining access to USAID information systems and annually thereafter.

b. 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.

c. Security and privacy refresher training must be completed on an annual basis by all contractor and subcontractor personnel providing support under this contract. USAID will provide notification and instructions on completing this training.

d. Contractor 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.

e. Within fifteen (15) calendar days of completing the initial IT security training, the contractor must notify the COR in writing that its employees, in performance of the contract, have completed the training. The COR will inform the contractor of any other training requirements.

4. Information Security and Privacy Incidents

a. 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. Contractor 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 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 Contractor's discovery of a spillage or security incident involving classified information, the Contractor must immediately (within 30 minutes) notify CIOHELPDESK@ 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 Contractor will abide by USAID instructions on correcting such a spill or security incident.

Contractor 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, Contractor 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 Contractor 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".

b. 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. Contractor 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: CIOHELPDESK@ 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".

c. Information Security Incident Response Requirements

i. All determinations related to Information Security and Privacy Incidents, associated with information Systems or Information maintained by the contractor in support of the activities authorized under this contract, 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 Contractor 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 Contractor and contractor 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 Contractor in support of the activities authorized by this contract will be made only by the USAID CIO through the CO or COR.

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

5. The Contractor shall immediately notify the Contracting Officer in writing whenever it has reason to believe that the terms and conditions of the contract may be affected as a result of the reported incident.
6. The Contractor 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 CIOHELPDESK@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.

H.30 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION 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 the authorizing official is 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 Contractor, its subcontractors, and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") 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 contractor shall be responsible for implementing information security for all information systems procured, developed, deployed, and/or operated on behalf of the US Government. All Contractor personnel performing under this contract and Contractor 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, EGovernment 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 Contractor 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 FIPS 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 Contractor 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 Contractor's products to be tested within a USAID or third party test facility to show compliance with this requirement.

(3) Secure Configurations

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

(5) Security Monitoring, Auditing and Alerting Requirements: All Contractor owned and operated systems that use or store USAID information must meet or exceed standards documented in this contract and in Service Level Agreements and Memorandums of Understanding/Agreements pertaining to security monitoring and alerting. These requirements include but are not limited to: Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEV-FAR-18-2c, and M/OAA-DEV-AIDAR-18-2c) 29 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) Contractor System Oversight/Compliance

i. The federal government has the authority to conduct site reviews for compliance validation. Full cooperation by the Contractor is required for audits and forensic analysis.

ii. The Contractors must afford USAID the level of physical or logical access to the Contractor'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 Contractor 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 Contractor 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. Alternatively, the Contractor may allow USAID information security staff to run scans directly.

iv. The Contractors 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 contract, the Contractor 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, 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 contractor must obtain an Authority to Operate (ATO) signed by a USAID Authorizing Official from the contracting officer or COR. The Contractor 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 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 Contractor 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 Contractor 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 contractor 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 Contractor must submit a signed SA&A package approved by the 3PAO to USAID at saacapackages@usaid.gov at least 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 Contractor 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 Contractor must submit SA&A packages to the CIO at least sixty (60) days prior to production or the expiration of the current ATO.
ix. Once the USAID Chief Information Security Officer or designee determines the risks, the Contractor 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 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 Contractor must provide timely responses as requested by USAID and OMB.

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

H.31 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.
"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.
"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.

"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 Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") 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), EGovernment 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 Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract issued hereunder.

i. If authorized by the terms of this contract issued hereunder, any access to, or use or disclosure of, Federal information shall only be for purposes specified in this contract.

ii. The Contractor 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 contract.

(2) The Contractor 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 Contracting Officer.

(d) Records Management and Access to Information

(1) The Contractor 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 contract and National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Federal information, including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by the Contracting Officer in support of government compliance requirements to include but not limited to Freedom of Information Act, Privacy Act, e- Discovery, eRecords and legal or security investigations.

(3) The Contractor shall retain and maintain all Federal information in accordance with records retention provisions negotiated by the terms of the contract and in accordance with USAID records retention policies.

(4) The Contractor shall dispose of Federal information in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

(e) Notification of third party access to Federal information: The Contractor shall notify the Government 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 Contractor 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 Contractor's discovery of a spillage or security incident involving classified information, the Contractor shall immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or information security incident in compliance with agency-specific instructions. The Contractor will also notify the Contracting Officer or Contracting Officer's Representative and the Contractor Facilities Security Officer. The Contractor 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. Contractor employees must report via 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 Contracting Officer and Contracting Officer's representative and the Contractor Facilities Security Officer. Contractor 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, Contractor 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 Contractor must provide any supplementary information or reports related to a previously reported information security 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".

(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. Contractor employees must report by e-mail all Privacy Incidents to the USAID Service Desk immediately (within 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".

(i) Information Ownership and Rights: USAID information stored in a cloud environment remains the property of USAID, not the Contractor 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 contract. Further, 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 Contractor 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 Contractor 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 Contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.FedRAMP.gov.

(3) The Contractor 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 Contractor must make available to the Contracting Officer, the most

current, and any other, Security Assessment Reports for consideration as part of the Contractor'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 Contractor 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 Contractor's implementation as documented in the Security Assessment Report must be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT) (Class Deviations M/OAA-DEVFAR- 18-2c, and M/OAA-DEV-AIDAR-18-2c) 37 Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.
(6) The Contractor 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 Contractor 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 Contractor 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 Contractor solution. The Contractor 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 Contractor must disclose the data server locations where the Agency data will be stored as well as the redundant server locations. The Contractor must have prior Agency approval to store Agency data in locations outside of the United States.

(m) Terms of Service (ToS): The Contractor must disclose any requirements for terms of service agreements and clearly define such terms prior to contract award. All ToS provisions regarding controlling law, jurisdiction, and indemnification must align with Federal statutes, policies, and regulations.

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; 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 Contractor 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 Contractor must route all USAID traffic through the TIC. Clauses And Special Contract Requirements For Facilities Access, Security, and Information Technology (IT)

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

(1) The Contractor must ensure appropriate forensic tools can reach all devices based on an approved timetable.
(2) The Contractor must not install forensic software or tools without the permission of USAID.
(3) The Contractor, 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 contract.
(4) The Contractor, in coordination with USAID M/CIO/IA, must clearly define capabilities, procedures, roles and responsibilities and tools and methodologies for these activities.

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

I.2 52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) *Definitions*. As used in this clause--

"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
"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 system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
"Safeguarding" means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements*. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

I.3 52.204-23 - PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)

(a) Definitions.

As used in this clause—Covered article means any hardware, software, or service that—

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided in whole in part by a covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a covered entity.

Covered entity means—

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

(b) Prohibition.

Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115–

91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing any covered article that the Government will use on or after October 1, 2018; and

(2) Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) Reporting requirement.

(1) In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i) Within 1 business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d) Subcontract
The subcontractor shall insert the substance of this clause, including this paragraph (d) in all subcontract
including subcontracts for the acquisition of commercial items."

I. 4 52.215-19 NOTIFICATION OF OWNERSHIP CHANGES (OCT 1997)

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 days.

(2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall --

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

I.9 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (OCT 2015)

(a) *Definitions*. As used in this clause—
"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran,' and "recently separated veteran" have the meanings given at FAR 22.1301.

(b) *Equal opportunity clause*. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $150,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate of identify properly the parties and their undertakings.

I.10 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)

(a) *Equal opportunity clause.* The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60.741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) *Subcontracts.* The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of $15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

FAR 52.204-24: Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v) of the provision at 52.212-3, Offeror Representations and Certifications-Commercial Items.

(a) Definitions. As used in this provision—
Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition.
(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use

of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) Representation. The Offeror represents that—

(1) **It □ will, □ will not provide** covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that**— It □ does, □ does not use** covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) Disclosures. (1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

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

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

"Covered foreign country" means The People's Republic of China.

"Covered telecommunications equipment or services" means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

"Critical technology" means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled (i) Pursuant to

multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or (ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

"Substantial or essential component" means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) *Prohibition.* Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) *Exceptions.* This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

END OF SECTION I

Date of Offer:

Name of Offeror:

Typed Name and Title:

Signature_____Date:

ANNEX D

Certification Regarding Debarment, Suspension, or Proposed Debarment

By signing and submitting this certification, the offeror certified that neither it nor any of its Principals are ( ) are not ( ) presently debarred, suspended, proposed for debarment, or otherwise declared ineligible from participation in this transaction by any Federal department or agency.

Vendor Name: _____

Signatures: _____

Signatory Name: _____

Signatory Title: _____

Date: _____

ANNEX E

See attached excel template