CADMUS

REQUEST FOR PROPOSALS (RFP)

Digital Agriculture Ecosystem Assessments

TO:	Potential Offerors
FROM:	The Cadmus Group USAID Digital Forward Mechanism
ISSUANCE DATE:	June 25, 2024
DEADLINE FOR QUESTIONS:	July 2, 2024, 17:00 EDT
SUBMISSION DATE:	July 15, 2024, 17:00 EDT

USAID Digital Forward is a five-year project that aims to drive the implementation of the USAID Digital Strategy across the Agency's multiple technical and regional sectors but also allows for operating unit buy-in for digital development activities that are aligned with objectives presented in the Strategy. This commitment is set out in USAID's 2020-2024 Digital Strategy. The goal of the Strategy is to "achieve and sustain open, secure, and inclusive digital ecosystems that contribute to broad-based, measurable development and humanitarian assistance outcomes." USAID works to achieve this goal through two overarching objectives: 1) improve measurable development and humanitarian assistance outcomes through the responsible use of digital technology in USAID programming; and 2) strengthen the openness, inclusiveness, and security of country digital ecosystems.

Cadmus is the prime implementor under the U.S. Agency for Digital Forward. Cadmus intends to award a **firm fixed price** contract for this activity with an estimated start date in September 2024.

This RFP is open to qualified companies and organizations with experience in similar activities as defined in the technical instructions.

Technical and price proposal requirements, as well as proposal evaluation criteria, are outlined in **Annex A**. Cadmus intends to make a contract award to the responsible Offeror(s) whose proposal(s) represents the best value to the U.S. government. More than one award may be made.

Proposals are due in electronic copy only, in MS Word, MS Excel, and/or PDF formats, by July 15, 2024, 17:00 EDT. Tables or charts in MS Excel format should be labeled appropriately. The email must not exceed 5MB in size. Technical and price proposals need to be submitted in separate electronic files and emailed to DFWDHO@cadmusgroup.com.

Price proposals shall include filled out and signed documentation attached in **Annexes D, E, and F**. All offerors shall also review information included in **Annex G** (relevant regulations).

Questions regarding this RFP are due in electronic copy by July 2, 2024, 17:00 EDT. They must be emailed (no phone questions will be accepted) to **dfwdho@cadmusgroup.com.** Potential Offerors who do not submit

questions shall send an email with their contact information if they wish to receive copies of answers. All questions and responses will be circulated to all offerors who ask questions and to those who register.

This RFP, including this cover letter, in no way obligates Cadmus to award a contract nor does it commit Cadmus to pay for any costs incurred in the preparation and submission of a proposal in response hereto. Furthermore, Cadmus reserves the right to reject any and all offers, if such an action is considered to be in the best interest of Cadmus and/or USAID.

CONTENTS

I. Introduction and Purpose

Estimated Start Date: August 2024

1.1 Activity Background

USAID Digital Forward is a five-year project that aims to drive the implementation of the USAID Digital Strategy across the Agency's multiple technical and regional sectors but also allows for operating unit buy-in for digital development activities that are aligned with objectives presented in the Strategy. This commitment is set out in USAID's 2020-2024 Digital Strategy. The goal of the Strategy is to "achieve and sustain open, secure, and inclusive digital ecosystems that contribute to broad-based, measurable development and humanitarian assistance outcomes." USAID works to achieve this goal through two overarching objectives: 1) improve measurable development and humanitarian assistance outcomes through the responsible use of digital technology in USAID programming; and 2) strengthen the openness, inclusiveness, and security of country digital ecosystems.

1.2 Purpose

Cadmus, the implementer of the USAID-funded Digital Forward mechanism, invites qualified offerors to submit proposals to provide technical assistance to the Bureau for Resilience, Environment, and Food Security (REFS) in its ongoing support of several USAID Missions through Digital Agriculture Ecosystem Assessments. Offerors will submit proposals to conduct Digital Agriculture Ecosystem Assessments in support of up to three USAID Missions to better understand, work with, and support the country's respective digital agriculture ecosystem to meet their development objectives. Offerors can apply for one, multiple, or all three requested Assessments. A budget range of $40,000-$55,000 with a level of effort of 70-115 days is anticipated for each Assessment. Offerors are encouraged to propose the most cost-effective solution for SOW implementation. Cost will be an evaluation factor.

1.3 Type of Award Anticipated

Cadmus anticipates awarding a Firm Fixed Price contract. This contract type is subject to change during negotiations. A Firm Fixed Price Contract is: An award for a total firm fixed price, for the provision of specific services, goods, or deliverables and is not adjusted if the actual costs are higher or lower than the fixed price amount.

Offerors are expected to include all costs, direct and indirect, into their total proposed price.

II. General Instructions

"Offeror", "Contractor", and/or "Bidder" means a firm proposing the work under this RFP. "Offer" and/or "Proposal" means the package of documents the firm submits to propose the work.

Offerors wishing to respond to this RFP must submit proposals, in English, in accordance with the following instructions. Offerors are required to review all instructions and specifications contained in this RFP. Failure to do so will be at the Offeror's risk. If the solicitation is amended, then all terms and conditions not modified in the amendment shall remain unchanged.

Issuance of this RFP in no way obligates Cadmus to award a contract or purchase order. Offerors will not be reimbursed for any costs associated with the preparation or submission of their proposal. Cadmus shall in no case be responsible for or liable for these costs.

Proposals are due no later than July 15, 2024 at 5pm EDT, to be submitted via email to DFWDHO@cadmusgroup.com. Please include the RFP number (REFS 2024-01) in the subject line of the email. Late offers will be rejected except under extraordinary circumstances at Cadmus' discretion. Technical proposals are limited to 10-14 pages, depending on the number of Assessments the bidder is applying for. This page limit excludes:

- Cover Letter;
- Workplan;
- Past Performance Examples;
- CVs (up to 2 pages each);

The submission to Cadmus of a proposal in response to this RFP will constitute an offer and indicates the Offeror's agreement to the terms and conditions in this RFP and any attachments hereto.

2.1 Proposal Cover Letter

A cover letter shall be included with the proposal on the Offeror's company letterhead with a duly authorized Signature. The cover letter shall include the following items:

- The Offeror will certify a validity period of 90 days for the prices provided.
- Acknowledge any solicitation amendments received.
- Include which of the three Assessments Offeror is applying to.

2.2 Questions regarding the RFP

Each Offeror is responsible for reading and complying with the terms and conditions of this RFP. Requests for clarification or additional information must be submitted in writing via email to DFWDHO@cadmusgroup.com by July 2 at 5pm EDT. No questions will be answered by phone. Copies of questions and responses will be distributed via email to all prospective bidders who are on record as having received this RFP after the submission date specified in the Synopsis above.

III. Instructions for the Preparation of Technical Proposals

Technical proposals shall be in a separate attachment from cost proposals and shall be clearly labeled as "VOLUME I: TECHNICAL PROPOSAL". Technical proposals are limited to 15 pages, excluding workplan, CVs of proposed personnel, past performance examples and cover letter.

This RFP is for the implementation of between one and three Digital Agriculture Ecosystem Assessments. Offerors may apply to implement only one Assessment, two assessments, or all assessments. Proposals should make it very clear the Assessments for which the Offeror is applying. Technical proposals shall include the following contents:

Technical Approach and Implementation Plan

- Narrative summary of firm's implementation plan, demonstrating that the Offeror is qualified to implement the SOW and achieve the deliverables according to the timeline.
    - Include country-specific plans for each country firm is interested in conducting Assessments for (maximum 2 pages per country, included in the overall page limit).
    - Workplan for overall implementation that includes specific activities for each country to which the bidder is applying, as relevant (not included in the overall page limit).

Past Performance

- Included as a section within the Implementation plan, offers should include a Past Performance section which provides a narrative summary of previous work of similar scope highlighting country- specific experience for the country Assessment(s) for which the Offeror is applying. Country- specific past performance narrative summaries should be a half-page to one page maximum per country assessment applying to.
- Past performance examples of reports of similar scope, if relevant. Past performance examples should only be shared if directly relevant (i.e., Assessment Reports of similar scope) (not counted in the proposal page limit).

Personnel Plan and Qualifications

- Included as a section within the Implementation plan, offers should include a Personnel Plan that includes titles and job responsibilities of proposed team, demonstrating its ability to coordinate efforts to successfully achieve the SOW. Plans should include any overarching team members across the Assessments as well as specify per-country teams.
    - Offerors are required to include, at a minimum, one local team member for each different Assessment country for which the Offeror is applying, with total local presence consisting of at least 65% of the total proposed level of effort (excluding copy editing and design). Offerors who are not able to meet this requirement can submit an alternative plan and justification, which will be considered. Preference will be given to Offerors that meet this threshold.
    - Preference will be given to Offerors that include at least one member of the team with gender and/or inclusive development expertise.
- CVs of proposed personnel that demonstrate relevant qualifications for the SOW.

3.1 Scope of Work

The objective of this activity is to carry out Digital Agriculture Ecosystem Assessments in support of up to three USAID Missions to better understand, work with, and support the country's respective digital agriculture ecosystem to meet their development objectives. The assessment recommendations will be used to help inform both current and future programming. The following are key to the Assessments:

- A stakeholder mapping of the relevant actors within the Digital Agriculture Ecosystem within each country of focus, with a particular focus on local actors.
- Identification of key challenges and opportunities for more effectively leveraging digital technologies in the agriculture and aligned sectors among the different stakeholders within each country's ecosystem, consistent with each Mission's and USAID's priorities.[1]
- Identification of relevant local actors that the Mission can potentially work with to support the implementation of any recommendations identified through the assessment.
- Identification of key challenges and opportunities specific to marginalized and underrepresented groups (also considering gender, age, ethnicity, socio-economic status and other intersecting disadvantage as relevant) in the agriculture and aligned sectors within each countries' context and incorporation of an inclusive development lens to the deliverables.[2]
- A local presence in the focus country by, at minimum, one Assessment team member with total local presence consisting of at least 65% of the total proposed level of effort (excluding copy editing and design).

The scopes of work for this activity (three countries) are in Attachments A, B, and C.

3.2 Tasks

The Assessment is approximately a 4-6 month engagement (dependent on country context, time zone, and in-country travel considerations) and contains three phases: 1) desk research and planning, 2) interviews, and 3) analysis and report writing. In-country travel and in-person interviews should be scheduled if restrictions due to the local security context allows. International travel is not expected as part of this assignment. The support and tasks detailed below are based on this assumption.

1. TASK 1: Desk Research & Assessment Planning The goal is to obtain baseline knowledge to enter the interview phase well-informed about the country context and what gaps need to be filled. During this phase interviewee identification and outreach is initiated. The following illustrative tasks may take place during this phase:

[1] Assessments should be aligned with the Mission's Country Development Cooperation Strategy (CDCS), Global Food Security Strategy, USAID Climate Strategy, USAID Digital Strategy, RFS Digital Strategy Action Plan, and priorities around localization and inclusive development, as relevant and appropriate.

[2] USAID defines marginalized groups as follows: "People who are typically denied access to legal protection or social and economic participation and programs (i.e., police protection, political participation, access to healthcare, education, employment), whether in practice or in principle, for historical, cultural, political, and/or other contextual reasons. Such groups may include, but are not limited to, women and girls, persons with disabilities, LGBTI people, displaced persons, migrants, indigenous individuals and communities, youth and the elderly, religious minorities, ethnic minorities, people in lower castes, and people of diverse economic class and political opinions. These groups often suffer from discrimination in the application of laws and policy and/or access to resources, services, and social protection, and may be subject to persecution, harassment, and/or violence. They may also be described as "underrepresented," "at-risk," or "vulnerable"."

- Conduct an initial kick-off meeting with Mission staff to understand better the focus and outcomes they're seeking in addition to making relevant ecosystem connections. Confirming the plan across the teams including timing for milestone deadlines.
- Review of each focus Mission's Country Development Cooperation Strategy (CDCS, FTF Global Food Security Strategy GFSS Country Strategy), and current programs to identify USAID staff, USAID projects, and implementing partner staff that may have helpful insights and/or relationships with relevant ecosystem stakeholders.
- Develop a list of organizations and individuals to be interviewed with explicit attention to groups that represent or serve women, youth and marginalized groups.
- Develop a survey of USAID, implementing partners, donors, and/or Government staff for further insights and information.
- Organizing logistics for the interview phase, and meeting arrangements or teleconference details, as relevant.
- A summary of information on internet usage, mobile network coverage, and digital financial services uptake throughout the country as relevant to the ecosystem.
- Review of prior assessments or reports related to digitalization of the agriculture ecosystems that have been conducted by the Government, consulting firms, donors, or USAID programs or partners.
- Review of USAID digital agriculture ecosystem assessment guide. Selected firms are expected to use this guide, which includes sample survey and KII questions, as the foundation of their approach, although they are welcome to propose modifications or enhancements to the assessment methodology to meet the on-the-ground context. The guide is not currently publicly available. It will be shared with the selected firm/s after agreement execution.
- Identify any resources related to the digital divide as relevant to USAID agricultural programming in each country.

Deliverables:

- Final workplan (GANTT chart)
- In-brief to the Mission and REFS team (and others as requested) to share initial findings from background research, invite team members to participate in scheduled meetings, and to solicit final input and feedback.
- List of potential key informants to be interviewed, organized by role within the ecosystem (including digital solution providers, farmer organizations, cooperatives, government agencies, NGOs, donors, financial institutions, academia, mobile network operators, agribusinesses, and other relevant actors)
- A summary of other donor activities within the digital agriculture ecosystem
- Draft schedule for virtual/in person assessment interviews

2. TASK 2: Virtual & In Person Assessments

Based on the desk research and available networks, identify and conduct outreach to key informants to schedule interviews. Based on stakeholder mapping and synthesis exercises identify knowledge gaps and target interviewee outreach. Specific tasks may include:

- Identifying, organizing, and scheduling initial interviews with key informants including stakeholders from the country government, regulators, other donors, implementing partners/other international development organizations, private sector, civil society, and academia, with a lens toward diversity among stakeholders.
- Collect and manage detailed contact information for key informants.
- Leading the interviews.
- Inviting Mission staff to participate in interviews, as interested and available.

Deliverables

- Mid-way synthesis presentation to Mission and REFS team on key findings, initial recommendations, any information gaps, and additional research needs, as necessary.
- Interview notes

3. TASK 3: Analysis, Assessment Reports & Presentations

The last phase includes writing a report that brings together the desk research, findings from the interviews, and specific actionable recommendations for how the Mission(s) can integrate digital into their programming and processes to meet their development objectives. Specific tasks include:

- Facilitating a post-interview synthesis session with the Mission and REFS team to identify key themes and potential recommendations.
- Communicating with the USAID Mission throughout the drafting phase to ensure findings and, in particular, recommendations align with Mission priorities, capacity, and plans.
- Coordinating with the Digital Forward Team throughout the report writing process for clearances and finalizing both the internal and external reports for publishing.
- Engaging a copy editor and graphic designer for basic report/presentation formatting.
- Coordinating with the USAID to schedule a presentation, as relevant.

Deliverables

- Draft version of the report in Google Docs
- Two versions of the report may be published based on Mission preference: internal USAID (as Google Doc), and external (as PDF).
- List of digital agriculture services and relevant donor funded projects in the country
- Interviewee contact list and final interview schedule (may be included as an Annexes to the report)
- Summary presentation deck in Google Slides with key findings and recommendations from the assessment per the Mission's requirements.

3.3 Program Task Milestones

TASK MILESTONES	TIMING
Desk Research and Planning	4-5 weeks
Key Informant Interviews	7 - 10 weeks
Analysis and Writing Draft Report	14 - 18 weeks
Final Report, Presentation and Clearance	16 - 19 weeks

Detailed Program Milestones

The below timelines are illustrative and will be finalized in consultation with each USAID Mission.

Deliverable	Estimated Due Date
Project In-Brief	Week 1
Final work plan (GANTT chart)	Week 2
Phase 1: Desk Research and Planning	
Initial ecosystem stakeholder mapping list	Week 4-5

A summary of other donor activities within the digital agriculture ecosystem	Week 4-5
Draft schedule for virtual/in person assessment interviews	Week 4-5
Interview Guides and Surveys, approved by Digital Forward and USAID	Week 4-5
Phase 2: Interviews	
Mid-way synthesis session for information gap identification and targeting of additional key informants, including USAID Mission staff if interested and available.	Week 5-7
Conduct interviews	Week 7-10
Phase 3: Analysis and Report Writing	
Draft report	Week 10-14
Final ecosystem stakeholder mapping list, interviewee contact list, and final interview schedule (may be included as an Annexes to the report)	Week 14-19
Final designed internal report	Week 14-19
Final designed external report	Week 14-19
Summary presentation deck with key findings from the assessment	Week 14-19

3.4 Technical Evaluation Criteria

Each proposal will be evaluated and scored against the evaluation criteria and evaluation sub-criteria, which are stated in the table below. Cost proposals are not assigned points, but for overall evaluation purposes of this RFP, technical evaluation factors other than cost, when combined, are considered approximately equal to cost factors. Proposals will be evaluated according to the following criteria:

Evaluation Criteria	Evaluation Sub-criteria	Maximum Points
Technical Approach and Implementation Plan	Implementation plan proposed by Offeror presents a credible approach towards the implementation of the SOW and the achievement of the deliverables in an independent manner, adaptive to client feedback, and within the specified timeline Country-specific plans that fully reflect the contextual nuance of each country, as it relates to the implementation of the SOW. Workplan demonstrates a thorough and logical plan to achieve SOW and deliverables by outlined timeline.	10 points

Past Performance	Past Performance section provides a narrative summary that demonstrates firm's capabilities to successfully take on projects of similar scope and size highlighting country-specific experience based on the specific country Assessments Offerors intend to implement. Past Performance section establishes Offeror's expertise in the sector. Past performance examples are directly relevant and demonstrate firm understands and can successfully undertake work of similar scope.	12 points
Personnel Plan and Qualifications	Personnel Plan demonstrating ability of proposed staff to successfully achieve the scope of work Personnel plan outlines job titles and responsibilities clearly demonstrates how the team will work together to achieve the scope of work. CVs of proposed personnel that demonstrate relevant qualifications for the SOW Proposed assessment teams per country include at least one locally based team member LOE of personnel plan includes local presence consisting of at least 65% of the total proposed level of effort (excluding copy editing and design).	12 points
Cost Proposal	Overall value of the bid Reality of proposed cost	10 points
	Total Points	44

IV. Instructions for the Preparation of Cost Proposals

Cost proposals shall be in a separate attachment from technical proposals and shall be clearly labeled as "VOLUME II: COST PROPOSAL."

4.1 Detailed Budget

Provided in Attachment C is a template for the cost proposal. Offerors shall complete the template including as much detailed information as possible. The Contractor is responsible for all applicable taxes and fees, as prescribed under the applicable laws for income, compensation, permits, licenses, and other taxes and fees due as required. The template should be considered guidance to ensure all costs are included. If the offeror's costs do not include all categories on the template, those that are not applicable do not need to be filled out. Conversely, if there are categories of costs not included in the current template, Offeror should add those costs.

4.2 Budget Narrative

The budget must have an accompanying budget narrative and justification that provides in detail the estimated costs for implementation of the SOW in Attachment A. The combination of the cost data and narrative must be sufficient to allow a determination of whether the costs estimated are reasonable. A budget narrative template is included in Attachment C.

V. Other Requirements

5.1 Language of the Contract

The language of the Contract is English.

5.2 Payment Structure

This will be a Firm Fixed Price contract, based on deliverables. The specific payment schedule per deliverable will be based on the proposed overall awarded budget, and will be negotiated at the time of award.

5.3 Damages for Delayed Performance

If any of the services performed do not confirm with Subcontract requirements, Contractor may require the Subcontractor to perform the services again in conformity with Subcontract requirements, for no additional price. If such deficiencies are not corrected in a timely manner, Contractor may cause the same to be corrected and deduct such corrective action costs incurred from monies otherwise due to the Subcontractor. The Subcontractor shall be liable for such excess costs and shall reimburse the Contractor within thirty (30) calendar days of receipt of invoice. This corrective action shall not limit the application of any other warranty or remedy available hereunder or by law. When the defects in services cannot be corrected by re-performance, the Contractor may require the Subcontractor to take necessary action to ensure that future performance conforms to Subcontract requirements. If the Subcontractor fails to promptly perform the services again or take the action necessary to ensure future performance in conformity with Subcontract requirements, Contractor may terminate the Subcontract for default. If the Subcontract is terminated for default and Contractor is forced to obtain the services from another vendor, Subcontractor may be liable for any additional procurement costs of those services from another provider.

5.4 Project Monitoring and Reporting

The Contractor shall propose a plan for project monitoring and reporting processes to meet the project objectives.

Throughout the duration of the project, the Contractor shall prepare and submit brief progress reports weekly to the Cadmus Digital Forward team.

5.5 Copyrights and Ownership

The Contractor warrants that it is not aware of any copyright, patent, trademark, trade secret or other proprietary right that it might infringe upon in providing the work required under the Technical Instructions. The Contractor shall indemnify and save Cadmus and Cadmus' Client harmless from any

and all claims, suits, liability, expense or damages for any alleged or actual infringement of any copyright, patent, trademark, trade secret or other proprietary right arising in connection with the work that the Contractor will provide.

Deliverables that will be first produced and submitted to USAID shall be the property of USAID. Additionally, any pre-existing item(s) either from the Contractor or Cadmus, shall remain the property of that party who created the item(s) throughout the life of the Contract, and said party shall retain all rights and privileges to ownership. Any item that is jointly developed during the course of the Contract shall be either owned by USAID or jointly owned by both parties.

All reports generated and data collected during this project shall not be reproduced, disseminated or discussed in open forum, other than for the purposes of completing the tasks described in this document. All findings, conclusions and recommendations shall be considered confidential and proprietary.

5.6 Estimated Award Timeline

Activity	**Estimated Dates**
- Request for proposals issued	June 25, 2024
- Deadline to submit questions	July 2, 2024, 17:00 EDT
- Deadline to submit offers	July 15, 2024, 17:00 EDT
- Expected start date	August 2024

5.7 Best and Final Offer (BAFO)

Cadmus reserves the right to proceed to a Best and Final Offer (BAFO) phase of the procurement process following the initial evaluation of proposals received in response to this Request for Proposal (RFP).

Upon completion of the initial evaluation, Cadmus may identify a subset of potential bidders whose proposals demonstrate exceptional merit and alignment with the project objectives. These selected bidders will be invited to participate in the BAFO phase.

The BAFO phase serves as an opportunity for selected bidders to revise and enhance their proposals, taking into account feedback provided during the initial evaluation process. Bidders may be requested to address specific concerns or provide further clarification on certain aspects of their proposals.

Bidders selected to participate in the BAFO phase will be notified in writing, detailing the rationale for their selection and providing guidance on the submission requirements and timeline for the revised proposals.

ANNEX A – Statement of Work: Guatemala

USAID/Guatemala is interested in understanding the impacts of COVID-19, climate change, and the global food security crisis stemming from Russia's war in Ukraine, on the local agriculture sector and how, if at all, digital technology has been and has the potential to be used to overcome/mitigate any of those impacts. The Mission would also like to better understand what is currently being done in the digital agriculture space in Guatemala, including a mapping of on-going or existing digital services that are nutrition, ag and market related, as well as a general sense of the mobile landscape, startup ecosystem and tech capacity in Guatemala. This should include private and non-profit efforts, as well as those led by the government, such as the Ministry of Agriculture's Registro Unico de Agricultores. Digital tools used to strengthen market access, capacity strengthening efforts related to online marketing, and digital financial services and artificial intelligence in the agriculture sector are all of particular interest to the Mission.

The assessment should include recommendations for how USAID/Guatemala can more effectively integrate digital services into its current and future Feed the Future programming, with a particular focus on the departments of Huehuetenango, Quiché, San Marcos, Quetzaltenango, Solola, Chimaltenango and Alta and Baja Verapaz. Current USAID activities of relevance for this assessment include Connecting Value Chains in the Verapaces, Scaling Agriculture Technologies, Rural Financial Inclusion, and Innovative Solutions for Agricultural Value Chains Project/PRO-INNOVA. The assessment should also include suggestions of relevant local actors that USAID/Guatemala can potentially work with to support the implementation of any recommendations identified through the assessment.

ANNEX B – Statement of Work: Burma

USAID Burma seeks a digital agriculture ecosystem country assessment which will map out the current digital conditions and propose recommendations to improve digital access, literacy, and security with a special focus on reach into ethnic areas. A deep analysis of the possibilities for digital technologies, including emerging technologies, such as artificial intelligence, in the agricultural sector will inform programming and improve the use of digital technology to achieve the Mission's Feed the Future and broader development objectives.

In an era of extreme accessibility issues brought on by the brutal and ongoing civil war, digital technologies in the agriculture sector in Burma have the potential to underpin broad sector support. This may include digital support to (including digital agricultural extension) artificial intelligence solutions, land preparation and soil management, on-farm management, post-harvest handling, food loss and waste management, market system management, agri-inputs value chain management and facilitation, logistics and transportation, access to finance, weather forecasting and climate change vulnerability, amongst others.

The Mission is particularly interested in the promotion of digital technologies and artificial intelligence solutions to reach smallholder farmers, particularly in ethnic areas around the perimeter of the country. In addition, the assessment should explore opportunities to facilitate sustainable and inclusive business models in the digital agriculture sector, including a focus on incentivizing participation of youth, women, and other marginalized groups. Last, the assessment should include a focus on the opportunities and challenges that exist for the Mission and its programming in relation to using and supporting the uptake of digital technologies.

ANNEX C – Statement of Work: Niger

Niger - USAID last conducted a digital agriculture assessment for Niger in 2019. Since then, the USG's investments in digital agriculture in Niger have had mixed results. The Legume Systems Innovation Lab has had success using SAWBO videos to provide hybrid extension services with the agents sharing videos in local languages to improve cowpea yields. A WhatsApp group of over 25,000 users shares videos regularly. The videos were also uploaded to the RECA repository, a private sector extension service with a large online collection of resources also accessible via multiple in-house apps. On the other hand, another project, implemented by Michigan State University to create an online marketplace for buyers and sellers of commodities to connect, negotiate, and purchase was not successful and no longer operates – although the Nigerian version was successful. MCC invested heavily in statistical capability for the Ministry of Agriculture and it was basically never used. However, its eVoucher program for subsidized fertilizer worked well in pilot sites with larger farmers. The Current and Emerging Threats Innovation Lab will promote the use of Plant Village to share real time information on crop risks. It remains to be seen if that platform is adopted and routinely used. Suffice it to say, digital extension seems to be a promising area that seems to be growing.

USAID/Niger routinely receives requests from the GoN, NGOS, and the government at all levels. However, the Mission has not noted requests for support to digital activities or digitization in agriculture, which is unlike other sectors, such as education. It would be helpful for the Mission to understand where digital technology has strong potential in the agriculture sector, and to help the Mission identify overlooked opportunities and predict growth rates for the sector. The Mission is interested in completing a landscaping assessment of the digital agriculture sector, including identifying the major actors and their relationship to one another. The assessment should examine existing digital policies in the GoN, primarily for agriculture, but also for related sectors such as energy, commerce, and education, and assess the degree to which they are actually implemented. It should identify capacity gaps in the digital agriculture sector, provide recommendations for areas of potential investment that might serve as a driver for economic growth, as well as recommendations for how the digital enabling environment, especially as it relates to agriculture, might be improved.

ANNEX D – Reps and Certs for Offeror

ANNUAL SUPPLIER REPRESENTATIONS and CERTIFICATIONS

Procurement of material, services and supplies for a United States Government contract requires that prime contractors, subcontractors, and suppliers comply with socioeconomic programs enacted into public law, implemented by Executive Order, and promulgated by Federal Regulations. Representations and Certifications must be completed prior to award of any order(s) to your company and be updated annually.

COMPANY NAME	
ADDRESS, PO BOX, SUITE NO.	
CITY, STATE, ZIP CODE	
PHONE	
FAX	
E-MAIL ADDRESS	
CAGE CODE	
UEI NUMBER	
NUMBER OF EMPLOYEES FOR LAST 12 MONTHS (FAR 52.212-3)	

NORTH AMERICAN INDUSTRIAL CLASSIFICATION SYSTEM (NAICS) CODE (FAR 19.102) NAICS Code listings are also available at your public library, and through the Internet at: http://www.sba.gov/regulations/sicco des/. of Provision)	Enter the 6-digit NAICS Code that most closely represents the product, commodity, or service that your firm is likely to sell to Nathan in the calendar year covered by these representations. NAICS Code:

Please review each statement below and place a check mark in the box that represents your current state of compliance with each requirement. **NOTE: DO NOT LEAVE ANY OF THE SECTIONS BLANK.** Sign and date the last page and return the completed form to the appropriate Nathan Procurement Compliance Office.

(End of provision)

REPORTING EXECUTIVE COMPENSATION AND FIRST TIER SUBCONTRACT AWARDS (FAR 52.204-10)

The following questions (1-3) apply to first tier sub-award recipients to US Federal Contracts only. If you are not a first-tier sub-award recipient, please skip this section and go to section 2.

1. In the previous tax year, was your company's gross income from all sources under $300,000?

YES ☐ NO ☐
(If your response to item 1 is "No", please skip questions 2 and 3 below and go to section 2)

2. In your preceding completed fiscal year, did you receive:
   a. 80% or more of annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements; **and**
   b. $25,000,000 or more in annual gross revenues from U.S. federal contracts, subcontracts, loans, grants, subgrants, and/or cooperative agreements?

YES ☐ NO ☐
(If your response to item 2 above is "No", please skip item 3 below and go to section 2)

3. Does the public have access to information about the compensation of the senior executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d), or section 6104 of the Internal Revenue Code of 1986?

YES ☐ NO ☐
Yes (if your response to item 3 is "Yes", go to section 2)
No (if your response to item 3 is "No", complete compensation information as indicated below)
Name: Position: Salary: (US Dollar)
Name: Position: Salary: (US Dollar)
Name: Position: Salary: (US Dollar)

Name: Position: Salary: (US Dollar)
Name: Position: Salary: (US Dollar)
Name: Position: Salary: (US Dollar)

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

As prescribed in 4.2105(b), insert the following clause:

PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

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

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (*e.g.*, connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (*e.g.*, fiber optic, coaxial cable, Ethernet).

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).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (*e.g.*, connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (*e.g.*, voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

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

(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. 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 FAR 4.2104.

(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, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. 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.

(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) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

Covered Telecommunications Equipment or Services-Representation. 52.204-26
Section 889(a)(1)(A) of Public Law 115-232.

(1) 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".

(2) The Offeror represents that it □ does, □ 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.

(End of Provision)

CERTIFICATION REGARDING RESPONSIBILITY MATTERS 52.204-26

Certification Regarding Responsibility Matters (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals–

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

(2) □ Have, □ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

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

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

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

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

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

(ii) *Examples*.

(A) 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.

(B) 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.

(C) 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.

(D) 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).

52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS

- Supplier represents and certifies that it is a small business concern ☐ Yes ☐ No

Complete only if Supplier represented itself as a small business concern:

Women-owned small business concern (FAR 52.219-8).	☐ Yes ☐ No
Veteran-owned small business concern (FAR 52.219-8).	☐ Yes ☐ No
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 (FAR 52.219-8).	☐ Yes ☐ No
Small disadvantaged business concern as defined in 13 CFR 124 (FAR 52.219-8).	☐ Yes ☐ No

- Ownership, please select all that apply

☐ Black American	☐ Hispanic American
☐ Subcontinent Asian American (persons with origins from India, Pakistan, Bangladesh, Sri Lanka, Bhutan, the Maldives Islands, or Nepal).	☐ Asian-Pacific American (persons with origins from Burma, Thailand, Malaysia, Indonesia, Singapore, Brunei, Japan, China, Taiwan, Laos, Cambodia (Kampuchea), Vietnam, Korea, The Philippines, U.S. Trust Territory of the Pacific Islands (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).
☐ Native American	☐ Other

- North American Industry Classification System (NAICS) (www.naics.com)

Supplier's NAICS CODE	Small business size standard
NAICS	Size

HISTORICALLY BLACK COLLEGE OR UNIVERSITY AND MINORITY INSTITUTION REPRESENTATION (52.226-2)

- The Offeror represents that it is a historically black college or university ☐ Yes ☐ No

CERTIFICATION REGARDING KNOWLEDGE OF CHILD LABOR FOR LISTED END PRODUCTS (FAR 52.222-18)

[An award will not be made to an OFFEROR unless the Offeror, by checking the appropriate block, certifies to either paragraph (a) or (b) of this provision.]

a. [☒] OFFEROR will not supply any end product listed in paragraph C that was mined, produced, or manufactured in a corresponding country as listed for that end product.

PLEASE NOTE: If A is selected, please indicate NONE under "Listed End Product" and "Listed Countries of Origin" in Section C.

b. [☐] OFFEROR may supply an end product listed in paragraph C that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture such end product. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

c. Listed End Product

Listed Countries of Origin

PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (FAR 52.209-6)

a. The Government suspends or debars Contractors to protect the Government's interests. Other than a subcontract for a commercially available off-the-shelf item, the Contractor shall not enter into any subcontract, in excess of $30,000 with a Contractor that is debarred, suspended, or proposed for debarment by any executive agency unless there is a compelling reason to do so.
b. The Contractor shall require each proposed subcontractor whose subcontract will exceed $30,000, other than a subcontractor providing a commercially available off-the-shelf item, to disclose to the Contractor, in writing, whether as of the time of award of the subcontract, the subcontractor, or its principals, is or is not debarred, suspended, or proposed for debarment by the Federal Government.
c. A corporate officer or a designee of the Contractor/Subcontractor shall notify the Contracting Officer, in writing, before entering into a subcontract with a party (other than a subcontractor providing a commercially available off-the-shelf item) that is debarred, suspended, or proposed for debarment (see FAR 9.404 for information on the System for Award Management (SAM) Exclusions). The notice must include the following:
    1. The name of the subcontractor.
    2. The Contractor's knowledge of the reasons for the subcontractor being listed with an exclusion in SAM.
    3. The compelling reason(s) for doing business with the subcontractor notwithstanding its being listed with an exclusion in SAM.
    4. The systems and procedures the Contractor has established to ensure that it is fully protecting the Government's interests when dealing with such subcontractor in view of the specific basis for the party's debarment, suspension, or proposed debarment. (d) Subcontracts. Unless this is a contract for the acquisition of commercial items, the Contractor shall include the requirements of this clause, including this paragraph (e) (appropriately modified for the identification of the parties), in each subcontract that—
        i. Exceeds $30,000 in value; and
        ii. Is not a subcontract for commercially available off-the-shelf items as defined in FAR 52.209-6.

(End of Provision)

52.222-50 Combating Trafficking in Persons.

As prescribed in 22.1705 (a)(1), insert the following clause:

COMBATING TRAFFICKING IN PERSONS (OCT 2020)

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

Agent means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.

Coercion means-
(1) Threats of serious harm to or physical restraint against any person;
(2) Any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or
(3) The abuse or threatened abuse of the legal process.

Commercial sex act means any sex act on account of which anything of value is given to or received by any person.
(1) Any item of supply (including construction material) that is-
(i) A commercial item (as defined in paragraph (1) of the definition at FAR 2.101);
(ii) Sold in substantial quantities in the commercial marketplace; and
(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

"Commercially available off-the-shelf (COTS) item" means-

Debt bondage means the status or condition of a debtor arising from a pledge by the debtor of his or her personal services or of those of a person under his or her control as a security for debt, if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined.

Employee means an employee of the Contractor directly engaged in the performance of work under the contract who has other than a minimal impact or involvement in contract performance.

Forced Labor means knowingly providing or obtaining the labor or services of a person-
(1) By threats of serious harm to, or physical restraint against, that person or another person;
(2) By means of any scheme, plan, or pattern intended to cause the person to believe that, if the person did not perform such labor or services, that person or another person would suffer serious harm or physical restraint; or
(3) By means of the abuse or threatened abuse of law or the legal process.

Involuntary servitude includes a condition of servitude induced by means of-
(1) Any scheme, plan, or pattern intended to cause a person to believe that, if the person did not enter into or continue in such conditions, that person or another person would suffer serious harm or physical restraint; or
(2) The abuse or threatened abuse of the legal process.

Recruitment fees means fees of any type, including charges, costs, assessments, or other financial obligations, that are associated with the recruiting process, regardless of the time, manner, or location of imposition or collection of the fee.
(1) Recruitment fees include, but are not limited to, the following fees (when they are associated with the recruiting process) for-
(i) Soliciting, identifying, considering, interviewing, referring, retaining, transferring, selecting, training, providing orientation to, skills testing, recommending, or placing employees or potential employees;
(ii) Advertising
(iii) Obtaining permanent or temporary labor certification, including any associated fees;
(iv) Processing applications and petitions;

(v) Acquiring visas, including any associated fees;

(vi) Acquiring photographs and identity or immigration documents, such as passports, including any associated fees;

(vii) Accessing the job opportunity, including required medical examinations and immunizations; background, reference, and security clearance checks and examinations; and additional certifications;

(viii) An employer's recruiters, agents, or attorneys, or other notary or legal fees;

(ix) Language interpretation or translation, arranging for or accompanying on travel, or providing other advice to employees or potential employees;

(x) Government-mandated fees, such as border crossing fees, levies, or worker welfare funds;

(xi) Transportation and subsistence costs-

(A) While in transit, including, but not limited to, airfare or costs of other modes of transportation, terminal fees, and travel taxes associated with travel from the country of origin to the country of performance and the return journey upon the end of employment; and

(B) From the airport or disembarkation point to the worksite;

(xii) Security deposits, bonds, and insurance; and

(xiii) Equipment charges.

(2) A recruitment fee, as described in the introductory text of this definition, is a recruitment fee, regardless of whether the payment is-

(i) Paid in property or money;

(ii) Deducted from wages;

(iii) Paid back in wage or benefit concessions;

(iv) Paid back as a kickback, bribe, in-kind payment, free labor, tip, or tribute; or

(v) Collected by an employer or a third party, whether licensed or unlicensed, including, but not limited to-

(A) Agents;

(B) Labor brokers;

(C) Recruiters;

(D) Staffing firms (including private employment and placement firms);

(E) Subsidiaries/affiliates of the employer;

(F) Any agent or employee of such entities; and

(G) Subcontractors at all tiers.

Severe forms of trafficking in persons means-

(1) Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or

(2) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

"Sex trafficking" means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.

Subcontract means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.

Subcontractor means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.

United States means the 50 States, the District of Columbia, and outlying areas.

(b) *Policy.* The United States Government has adopted a policy prohibiting trafficking in persons including the trafficking-related activities of this clause. Contractors, contractor employees, and their agents shall not-

(1) Engage in severe forms of trafficking in persons during the period of performance of the contract;

(2) Procure commercial sex acts during the period of performance of the contract;

(3) Use forced labor in the performance of the contract;

(4) Destroy, conceal, confiscate, or otherwise deny access by an employee to the employee's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority;

(5) (i) Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language understood by the employee or potential employee, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant costs to be charged to the employee or potential employee, and, if applicable, the hazardous nature of the work;

(ii) Use recruiters that do not comply with local labor laws of the country in which the recruiting takes place;

(6) Charge employees or potential employees recruitment fees;

(7) (i) Fail to provide return transportation or pay for the cost of return transportation upon the end of employment-

A. For an employee who is not a national of the country in which the work is taking place and who was brought into that country for the purpose of working on a U.S. Government contract or subcontract (for portions of contracts performed outside the United States); or
B. For an employee who is not a United States national and who was brought into the United States for the purpose of working on a U.S. Government contract or subcontract, if the payment of such costs is required under existing temporary worker programs or pursuant to a written agreement with the employee (for portions of contracts performed inside the United States); except that-

(ii) The requirements of paragraphs (b)(7)(i) of this clause shall not apply to an employee who is-

A. Legally permitted to remain in the country of employment and who chooses to do so; or
B. Exempted by an authorized official of the contracting agency from the requirement to provide return transportation or pay for the cost of return transportation;

(iii) The requirements of paragraph (b)(7)(i) of this clause are modified for a victim of trafficking in persons who is seeking victim services or legal redress in the country of employment, or for a witness in an enforcement action related to trafficking in persons. The contractor shall provide the return transportation or pay the cost of return transportation in a way that does not obstruct the victim services, legal redress, or witness activity. For example, the contractor shall not only offer return transportation to a witness at a time when the witness is still needed to testify. This paragraph does not apply when the exemptions at paragraph (b)(7)(ii) of this clause apply.

(8) Provide or arrange housing that fails to meet the host country housing and safety standards; or

(9) If required by law or contract, fail to provide an employment contract, recruitment agreement, or other required work document in writing. Such written work document shall be in a language the employee understands. If the employee must relocate to perform the work, the work document shall be provided to

the employee at least five days prior to the employee relocating. The employee's work document shall include, but is not limited to, details about work description, wages, prohibition on charging recruitment fees, work location(s), living accommodations and associated costs, time off, roundtrip transportation arrangements, grievance process, and the content of applicable laws and regulations that prohibit trafficking in persons.

(c) *Contractor requirements*. The Contractor shall-
(1) Notify its employees and agents of-

I. The United States Government's policy prohibiting trafficking in persons, described in paragraph (b) of this clause; and
II. The actions that will be taken against employees or agents for violations of this policy. Such actions for employees may include, but are not limited to, removal from the contract, reduction in benefits, or termination of employment; and

(2) Take appropriate action, up to and including termination, against employees, agents, or subcontractors that violate the policy in paragraph (b) of this clause.

(d) *Notification.*
(1) The Contractor shall inform the Contracting Officer and the agency Inspector General immediately of-

I. Any credible information it receives from any source (including host country law enforcement) that alleges a Contractor employee, subcontractor, subcontractor employee, or their agent has engaged in conduct that violates the policy in paragraph (b) of this clause (see also 18 U.S.C. 1351, Fraud in Foreign Labor Contracting, and 52.203-13(b)(3)(i)(A), if that clause is included in the solicitation or contract, which requires disclosure to the agency Office of the Inspector General when the Contractor has credible evidence of fraud); and
II. Any actions taken against a Contractor employee, subcontractor, subcontractor employee, or their agent pursuant to this clause.

(2) If the allegation may be associated with more than one contract, the Contractor shall inform the contracting officer for the contract with the highest dollar value.

(e) *Remedies.* In addition to other remedies available to the Government, the Contractor's failure to comply with the requirements of paragraphs (c), (d), (g), (h), or (i) of this clause may result in-

(1) Requiring the Contractor to remove a Contractor employee or employees from the performance of the contract;
(2) Requiring the Contractor to terminate a subcontract;
(3) Suspension of contract payments until the Contractor has taken appropriate remedial action;
(4) Loss of award fee, consistent with the award fee plan, for the performance period in which the Government determined Contractor non-compliance;
(5) Declining to exercise available options under the contract;
(6) Termination of the contract for default or cause, in accordance with the termination clause of this contract; or
(7) Suspension or debarment.

(f) *Mitigating and aggravating factors.* When determining remedies, the Contracting Officer may consider the following:

(1) *Mitigating factors*. The Contractor had a Trafficking in Persons compliance plan or an awareness program at the time of the violation, was in compliance with the plan, and has taken appropriate remedial actions for the violation, that may include reparation to victims for such violations.

(2) *Aggravating factors*. The Contractor failed to abate an alleged violation or enforce the requirements of a compliance plan, when directed by the Contracting Officer to do so.

(g) *Full cooperation*.

(1) The Contractor shall, at a minimum-

i. Disclose to the agency Inspector General information sufficient to identify the nature and extent of an offense and the individuals responsible for the conduct;
ii. Provide timely and complete responses to Government auditors' and investigators' requests for documents;
iii. Cooperate fully in providing reasonable access to its facilities and staff (both inside and outside the U.S.) to allow contracting agencies and other responsible Federal agencies to conduct audits, investigations, or other actions to ascertain compliance with the Trafficking Victims Protection Act of 2000 (22 U.S.C. chapter 78), E.O. 13627, or any other applicable law or regulation establishing restrictions on trafficking in persons, the procurement of commercial sex acts, or the use of forced labor; and
iv. Protect all employees suspected of being victims of or witnesses to prohibited activities, prior to returning to the country from which the employee was recruited, and shall not prevent or hinder the ability of these employees from cooperating fully with Government authorities.

(2) The requirement for full cooperation does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not-

i. Require the Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine;
ii. Require any officer, director, owner, employee, or agent of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; or
iii. Restrict the Contractor from-
   A. Conducting an internal investigation; or
   B. Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.

(h) *Compliance plan*.
(1) This paragraph (h) applies to any portion of the contract that-

i. Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and
ii. Has an estimated value that exceeds $550,000.

(2) The Contractor shall maintain a compliance plan during the performance of the contract that is appropriate-

i. To the size and complexity of the contract; and
ii. To the nature and scope of the activities to be performed for the Government, including the number of non-United States citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking in persons.

(3) *Minimum requirements*. The compliance plan must include, at a minimum, the following:

i. An awareness program to inform contractor employees about the Government's policy prohibiting trafficking-related activities described in paragraph (b) of this clause, the activities prohibited, and the actions that will be taken against the employee for violations. Additional

information about Trafficking in Persons and examples of awareness programs can be found at the website for the Department of State's Office to Monitor and Combat Trafficking in Persons at http://www.state.gov/j/tip/.

ii. A process for employees to report, without fear of retaliation, activity inconsistent with the policy prohibiting trafficking in persons, including a means to make available to all employees the hotline phone number of the Global Human Trafficking Hotline at 1-844-888-FREE and its email address at help@befree.org.

iii. A recruitment and wage plan that only permits the use of recruitment companies with trained employees, prohibits charging recruitment fees to the employees or potential employees and ensures that wages meet applicable host-country legal requirements or explains any variance.

iv. A housing plan, if the Contractor or subcontractor intends to provide or arrange housing, that ensures that the housing meets host-country housing and safety standards.

v. Procedures to prevent agents and subcontractors at any tier and at any dollar value from engaging in trafficking in persons (including activities in paragraph (b) of this clause) and to monitor, detect, and terminate any agents, subcontracts, or subcontractor employees that have engaged in such activities.

(4) *Posting*.

i. The Contractor shall post the relevant contents of the compliance plan, no later than the initiation of contract performance, at the workplace (unless the work is to be performed in the field or not in a fixed location) and on the Contractor's Web site (if one is maintained). If posting at the workplace or on the Web site is impracticable, the Contractor shall provide the relevant contents of the compliance plan to each worker in writing.

ii. The Contractor shall provide the compliance plan to the Contracting Officer upon request.

(5) *Certification*. Annually after receiving an award, the Contractor shall submit a certification to the Contracting Officer that-

i. It has implemented a compliance plan to prevent any prohibited activities identified at paragraph (b) of this clause and to monitor, detect, and terminate any agent, subcontract or subcontractor employee engaging in prohibited activities; and

ii. After having conducted due diligence, either-

A. To the best of the Contractor's knowledge and belief, neither it nor any of its agents, subcontractors, or their agents is engaged in any such activities; or

B. If abuses relating to any of the prohibited activities identified in paragraph (b) of this clause have been found, the Contractor or subcontractor has taken the appropriate remedial and referral actions.

(6) *Subcontracts*

(1) The Contractor shall include the substance of this clause, including this paragraph (i), in all subcontracts and in all contracts with agents. The requirements in paragraph (h) of this clause apply only to any portion of the subcontract that-

i. Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and

ii. Has an estimated value that exceeds $550,000.

(2) If any subcontractor is required by this clause to submit a certification, the Contractor shall require submission prior to the award of the subcontract and annually thereafter. The certification shall cover the items in paragraph (h)(5) of this clause.

(End of clause)

Signature of Certifying Official from Company:	
Name of Certifying Official from Company:	Click here to enter text.
Title of Certifying Official from Company:	Click here to enter text.
Date of Certification/Signature:	Click here to enter text.

ANNEX E – Certification Regarding Terrorist Financing

Firm Name:

Certification Regarding Terrorist Financing

By signing and submitting this application, the prospective recipient provides the certification set out below:

1. The Recipient, to the best of its current knowledge, did not provide, within the previous ten years, and will take all reasonable steps to ensure that it does not and will not knowingly provide, material support or resources to any individual or entity that commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated, or participated in terrorist acts, as that term is defined in paragraph 3.

2. The **following** steps may enable the Recipient to comply with its obligations under paragraph 1:

a. Before providing any material support or resources to an individual or entity, the Recipient will verify that the individual or entity does not (i) appear on the master list of Specially Designated Nationals and Blocked Persons, which list is maintained by the U.S. Treasury's Office of Foreign Assets Control (OFAC) and is available online at OFAC's website: http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx , or (ii) is not included in any supplementary information concerning prohibited individuals or entities that may be provided by USAID to the Recipient, or (iii) is not included in the exclusion list of System for Award Management website www.SAM.gov.

b. Before providing any material support or resources to an individual or entity, the Recipient also will verify that the individual or entity has not been designated by the United Nations Security (UNSC) sanctions committee established under UNSC Resolution 1267 (1999) (the "1267 Committee") [individuals and

entities linked to the Taliban, Usama bin Laden, or the Al Qaida Organization]. To determine whether there has been a published designation of an individual or entity by the 1267 Committee, the Recipient should refer to the consolidated list available online at the Committee's website.
c. Before providing any material support or resources to an individual or entity, the Recipient will consider all information about that individual or entity of which it is aware and all public information that is reasonably available to it or of which it should be aware.

d. The Recipient also will implement reasonable monitoring and oversight procedures to safeguard against assistance being diverted to support terrorist activity.

3. For purposes of this Certification

"Material support and resources" means currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel, transportation, and other physical assets, except medicine or religious materials."

b. "Terrorist act" means-
(i) an act prohibited pursuant to one of the 12 United Nations Conventions and Protocols related to terrorism (see UN terrorism conventions Internet site:

http://untreaty.un.org/English/Terrorism.asp); or

(ii) an act of premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents; or

(iii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

c. "Entity" means a partnership, association, corporation, or other organization, group, or subgroup.

d. References in this Certification to the provision of material support and resources shall not be deemed to include the furnishing of USAID funds or USAID-financed commodities to the ultimate beneficiaries of USAID assistance, such as recipients of food, medical care, micro-enterprise loans, shelter, etc., unless the Recipient has reason to believe that one or more of these beneficiaries commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated or participated in terrorist acts.

e. The Recipient's obligations under paragraph 1 are not applicable to the procurement of goods and/or services by the Recipient that are acquired in the ordinary course of business through contract or purchase, e.g., utilities, rents, office supplies, gasoline, etc., unless the Recipient has reason to believe that a vendor or supplier of such goods and services commits, attempts to commit, advocates, facilitates, or participates in terrorist acts, or has committed, attempted to commit, facilitated or participated in terrorist acts.

This Certification is an express term and condition of any agreement issued as a result of this application, and any violation of it shall be grounds for unilateral termination of the agreement by USAID prior to the end of its terms.

FIRM: _____

SIGNATURE: _____
NAME OF AUTHORIZED REPRESENTATIVE: _____
TITLE OF AUTHORIZED REPRESENTATIVE: _____
DATE:_____

ANNEX F – Evidence of Responsibility

Prime Contract # 720OAA23C00131

USAID Digital Forward

Subcontractor Evidence of Responsibility Statement

1. Authorized Negotiators

Click here to enter organization name's proposal for the Click here to enter program name may be discussed with any of the following individuals. These individuals are authorized to represent Click here to enter organization name in negotiation of this offer.

Click here to list names of authorized negotiators/signatories.

These individuals can be reached at Click here to enter organization name's office:

Click here to enter organization's address
Click here to enter organization's telephone number
Click here to enter organization's email address

2. Adequate Financial Resources - FAR 9.104-1(a)

Click here to enter narrative providing evidence that the Subcontractor possesses adequate financial resources to perform the subcontract, or the ability to obtain them.

3. Ability to Comply - FAR 9.104-1(b)

Click here to enter narrative providing evidence that the Subcontractor is able to comply with the proposed delivery or performance schedule, taking into consideration all existing commercial and governmental business commitments.

4. Record of Performance - FAR 9.104-1(c)

Click here to enter narrative providing evidence of Subcontractor's history of performance on previous and current contracts.

5. Record of Integrity and Business Ethics – FAR 9.104-1(d)

Click here to enter narrative providing evidence of Subcontractor's history and record of integrity and business ethics.

6. Organization, Experience, Accounting and Operational Controls, and Technical Skills FAR 9.104-1(e)

Click here to enter narrative statement providing evidence that Subcontractor has the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them, in order to be able to perform under the proposed subcontract and subcontract type. Include, as appropriate, elements such as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by Subcontractor.

7. Equipment and Facilities - FAR 9.104-1(f)

Click here to enter narrative statement providing evidence that Subcontractor has the necessary equipment and facilities, or ability to obtain them, to be able to perform under the proposed subcontract.

8. Eligibility to Receive Award - FAR 9.104-1(g) and 9.108

Click here to enter narrative statement regarding Subcontractor's eligibility to receive an award under applicable laws and regulations. Statement must include Subcontractor's current status with respect to being suspended or debarred, and whether or not Subcontractor is treated as an inverted domestic corporation under 6 U.S.C. 395(b), i.e., a corporation that used to be incorporated in the United States, or used to be a partnership in the United States, but is not incorporated in a foreign country, or is a subsidiary whose parent company is incorporated in a foreign country, that meets the criteria specified in 6 U.S.C. 395(b).

9. Cognizant Government Audit Agency

Click here to enter the Name, address, and phone number of Subcontractor's Cognizant Government Audit Agency. If Subcontractor does not have a NICRA and Cognizant Government Audit Agency, so state, and provide the Name, address, and phone number of Subcontractor's independent certified public accounting (CPA) firm.

10. Subcontractor's Unique Entity Identifier (UEI) and Employer Tax ID Numbers

Subcontractor's UEI Number: Click here to enter UEI number

Subcontractor's Employer Tax ID Number: Click here to enter Tax ID number

11. Subcontractor Certification

I hereby certify that the information contained in this Subcontractor Evidence of Responsibility Statement is true and correct to the best of my knowledge and belief.

Signature: _____

Name: _____

Title: _____

Date: _____

ANNEX G – Relevant Regulations

Limitation on Acquisition of Information Technology (APRIL 2018)(DEVIATION Nos M/OAA-DEV-FAR-20-3c and M/OAA-DEV-AIDAR-20-2c)(APRIL 2020)
AIDAR 752.228-3 Worker's Compensation Insurance (Defense Base Act) (DEC 1991) [(DEVIATION JUN 2022)] Class Deviation No. M-OAA-DEV-AIDAR-22-10c
EXECUTIVE ORDER ON TERRORISM FINANCING
PROHIBITION OF ASSISTANCE TO DRUG TRAFFICKERS
Contractor Access to USAID Facilities and USAID's Information Systems (APRIL 2018)(DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)
Restrictions Against Disclosure (MAY 2016) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)
Information Technology Approval (APRIL 2018) (DEVIATION NO. M-OAA-DEV-FAR-22-03c)
Media and Information Handling and Protection (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)
Privacy and Security Information Technology Systems Incident Reporting (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)
Skills and Certification Requirements for Privacy and Security Staff (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)
Security Requirements for Unclassified Information Technology Resources (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c
Cloud Computing (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

Limitation On Acquisition Of Information Technology (APRIL 2018) (DEVIATION Nos M/OAA-DEV-FAR-20-3c and M/OAA-DEV-AIDAR-20-2c) (APRIL 2020)

(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.

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts that include information technology or information technology services.
(c) The Contractor must not acquire information technology as defined in this clause without the prior written approval by the contracting officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology 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 through modification to the contract expressly specifying the information technology equipment, software, or services approved for purchase by the COR and the Agency CIO. The Contracting Officer will include the applicable clauses and special contract requirements in the modification.

(f) Except as specified in the contracting officer's written approval, the Government is not obligated to reimburse the Contractor for any costs incurred for information technology as defined in this clause.

(g) The Contractor must insert the substance of this clause, including this paragraph (g), in all subcontracts.

[End of Clause]

H.7 AIDAR 752.228-3 Worker's Compensation Insurance (Defense Base Act) (DEC 1991) [(DEVIATION JUN 2022)] Class Deviation No. M-OAA-DEV-AIDAR-22-10c

In addition to the requirements specified in (48 CFR) FAR 52.228-3, the Contractor agrees to the following:

(a) The Contractor agrees to procure Defense Base Act (DBA) insurance pursuant to the terms of the contract between USAID and USAID's DBA insurance carrier unless the Contractor has a DBA self insurance program approved by the Department of Labor or has an approved retrospective rating agreement for DBA. The rates and contact information for USAID's DBA insurance carrier are published in an Acquisition & Assistance Policy Directive found on USAID's website: https://www.usaid.gov/work-usaid/resources-for-partners. Alternatively, the Contractor can request the rates and contact information from the Contracting Officer.

(b) If USAID or the Contractor has secured a waiver of DBA coverage (see (48 CFR) AIDAR 728.305-70(a)) for Contractor's employees who are not citizens of, residents of, or hired in the United States, the Contractor agrees to provide such employees with worker's compensation benefits as required by the laws of the country in which the employees are working, or by the laws of the employee's native country, whichever offers greater benefits.

(c) The Contractor further agrees to insert in all subcontracts hereunder to which the DBA is applicable, a clause similar to this clause, including this sentence, imposing on all subcontractors alike requirement to provide overseas worker's compensation insurance coverage and obtain DBA coverage under the USAID requirements contract.

EXECUTIVE ORDER ON TERRORISM FINANCING

The Contractor is reminded that U.S. Executive Orders (including E.O. 13224) and U.S. law prohibit transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. FAR 25.701 prohibits agencies and their Contractors and subcontractors from acquiring any supplies or services from individuals or organizations, if any proclamation, Executive Order, Office of Foreign Assets Control (OFAC) regulations, or statute administered by OFAC would prohibit such a transaction. Accordingly, the Contracting Officer must check the U.S. Department of the Treasury's OFAC List to ensure that the names of the Contractor and proposed subcontractors (and individuals from those organizations who have been made known to them), are not on the list. Mandatory FAR clause 52.225-13 Restrictions on Certain Foreign Purchases is included by reference in Section I.1 of this contract. By accepting this contract, the Contractor acknowledges and agrees that it is aware of the list as part of its compliance with the requirements of that clause. This clause must be included in all subcontracts/sub-awards issued under this contract. Further information is available at: http://www.state.gov/j/ct/rls/other/des/122570.htm and https://www.treasury.gov/resourcecenter/sanctions/Programs/Documents/terror.pdf

PROHIBITION OF ASSISTANCE TO DRUG TRAFFICKERS

USAID reserves the right to terminate this Contract, to demand a refund or take other appropriate measures if the Contractor or sub awardees are found to have been convicted of a narcotics offense or to have been engaged in drug trafficking as defined in 22 CFR Part 140.

H.13 Contractor Access to USAID Facilities and USAID's Information Systems (APRIL 2018)) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) HSPD-12 and Personal Identity Verification (PIV). Individuals engaged in the performance of this award as employees, consultants, or volunteers of the contractor must comply with all applicable Homeland Security Presidential Directive-12 (HSPD-12) and Personal Identity Verification (PIV) procedures, as described below, and any subsequent USAID or Government-wide HSPD-12 and PIV procedures/policies.

(b) A U.S. citizen or resident alien engaged in the performance of this award as an employee, consultant, or volunteer of a U.S firm may obtain access to USAID facilities or logical access to USAID's information systems only when and to the extent necessary to carry out this award and in accordance with this clause. The contractor's employees, consultants, or volunteers who are not U.S. citizens or resident aliens as well as employees, consultants, or volunteers of non-U.S. firms, irrespective of their citizenship, will not be granted logical access to U.S. Government information technology systems (such as Phoenix, GLAAS, etc.) and must be escorted to use U.S. Government facilities (such as office space).

(c) (1) No later than five business days after award, the Contractor must provide to the Contracting Officer's Representative (COR) a complete list of employees that require access to USAID facilities or information systems.

(2) Before a contractor (or a contractor employee, consultant, or volunteer) or subcontractor at any tier may obtain a USAID ID (new or replacement) authorizing the individual routine access to USAID facilities in the United States, or logical access to USAID's information systems, the individual must provide two forms of identity source documents in original form to the Enrollment Office personnel when undergoing processing. One identity source document must be a valid Federal or State Government-issued picture ID. Contractors may contact the USAID Security Office to obtain the list of acceptable forms of documentation. Submission of these documents, to include documentation of security background investigations, is mandatory in

order for the Contractor to receive a PIV/Facilities Access Card (FAC) card and be granted access to any of USAID's information systems. All such individuals must physically present these two source documents for identity proofing at their enrollment.

(d) The Contractor must send a staffing report to the COR by the fifth day of each month. The report must contain the listing of all staff members with access that separated or were hired under this contract in the past sixty (60) calendar days. This report must be submitted even if no separations or hiring occurred during the reporting period. Failure to submit the 'Contractor Staffing Change Report' each month may, at USAID's discretion, result in the suspension of all logical access to USAID information systems and/or facilities access associated with this contract. USAID will establish the format for this report.

(e) Contractor employees are strictly prohibited from sharing logical access to USAID information systems and Sensitive Information. USAID will disable accounts and revoke logical access to USAID IT systems if Contractor employees share accounts.

(f) USAID, at its discretion, may suspend or terminate the access to any systems and/or facilities when a potential Information Security Incident or other electronic access violation, use, or misuse incident gives cause for such action. The suspension or termination may last until such time as USAID determines that the situation has been corrected or no longer exists.

(g) The Contractor must notify the COR and the USAID Service Desk at least five business days prior to the Contractor employee's removal from the contract. For unplanned terminations of Contractor employees, the Contractor must immediately notify the COR and the USAID Service Desk (CIOHELPDESK@usaid.gov or (202) 712-1234). The Contractor or its Facilities Security Officer must return USAID PIV/FAC cards and remote authentication tokens issued to Contractor employees to the COR prior to departure of the employee or upon completion or termination of the contract, whichever occurs first.

(h) The contractor is required to insert this clause including this paragraph (h) in any subcontracts that require the subcontractor, subcontractor employee, or consultant to have routine physical access to USAID space or logical access to USAID's information systems.

(End of Clause)

RESTRICTIONS AGAINST DISCLOSURE (MAY 2016)(DEVIATION NO. M-OAA-DEV-AIDAR-22-O6c)

(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.

END

Information Technology Approval (APRIL 2018) (DEVIATION NO. M-OAA-DEV-FAR-22-03c)

(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.

(End)

MEDIA AND INFORMATION HANDLING AND PROTECTION (APRIL 2018)(DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(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), 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) 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).

END

Privacy and Security Information Technology Systems Incident Reporting (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Definitions. As used in this special contract requirement- “Information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. “Sensitive Information” or “Sensitive But Unclassified” Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS-46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could

result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers, "Personally Identifiable Information (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.

(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), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

(c) Privacy Act Compliance

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).

(d) IT Security and Privacy Training

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

(2) The USAID Rules of Behavior and all subsequent updates apply to and must be signed by each user prior to gaining access to USAID facilities and information systems, periodically at the request of USAID. USAID will provide access to the rules of behavior and provide notification as required

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

(4) 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.

(5) 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.

(e) Information Security and Privacy Incidents

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

(i) 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 CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or security incident in compliance with agency-specific instructions. The 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".

(2) Privacy Incidents Reporting Requirements: Privacy Incidents may result in the unauthorized use, disclosure, or loss of personally identifiable information (PII), and can result in the loss of the public's trust and confidence in the Agency's ability to safeguard personally identifiable information. PII breaches may impact individuals whose PII is compromised, including potential identity theft resulting in financial loss and/or personal hardship experienced by the individual. 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: CIO-HELPDESK@usaid.gov, regardless of day or time, as well as the USAID Contracting Officer or Contracting Officer's representative and the Contractor Facilities Security Officer. If known, the report must include information on the format of the PII (oral, paper, or electronic.) The subject line shall read "Action Required: Potential Privacy Incident".

(3) Information Security Incident Response Requirements

(i) All determinations related to Information Security and Privacy Incidents, associated with information Systems or Information maintained by the 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.

(f) 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.

(g) 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 CIO-HELPDESK@usaid.gov. A copy of the correspondence shall be sent to the prime Contractor (or higher tier subcontractor) and the Contracting Officer referencing the ticket number provided by the CIO-HELPDESK.

(End)

Skills and Certification Requirements for Privacy and Security Staff (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(a) Applicability: This special contract requirements applies to the Contractor, its subcontractors and personnel providing support under this contract and addresses the Privacy Act of 1974 (5 U.S.C. 552a - the Act), the Federal Information Security Management Act of 2002 (FISMA, Public Law 107-347, 44 U.S.C. 3531-3536), and Federal Information Security Modernization Act (FISMA) of 2014 (FISMA, Public Law 113-283 44 U.S.C. 3531-3536, as amended).

(b) Contractor employees filling the role of Information System Security Officer and Information Security Specialists must possess a Certified Information Systems Security Professional (CISSP) certification at time of contract award and maintain their certification throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor employees must provide proof of their certification status upon request.

(c) Contractor employees filling the role of Privacy Analysts must possess a Certified Information Privacy Professional (CIPP) credential with either a CIPP/US or a CIPP/G at the time of the contract award and must maintain the credential throughout the period of performance. This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Contractor employees must provide proof of their certification status upon request.

(End)

H.21 Cloud Computing (APRIL 2018) (DEVIATION NO. M-OAA-DEV-AIDAR-22-06c)

(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), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

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

(1) The Contractor shall not access, use, or disclose Federal information 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. 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.

(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.

(End)

PART II – CONTRACT CLAUSES

I.1 NOTICE LISTING CONTRACT CLAUSES INCORPORATED BY REFERENCE

The following contract clauses pertinent to this section are hereby incorporated by reference (by Citation Number, Title, and Date) in accordance with the clause at FAR "52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)". This contract incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available.

The full text of a clause may also be accessed electronically at this/these address(es): (FAR) FAR | Acquisition.GOV and (AIDAR) http://www.usaid.gov/ads/policy/300/aidar

52.202-1 Definitions
52.203-3 Gratuities
52.203-5 Covenant Against Contingent Fees
52.203-6 Restrictions on Subcontractor Sales to the Government
52.203-7 Anti-Kickback Procedures
52.203-8 Cancellation, Rescission, and Recovery of Funds for illegal or Improper Activity
52.203-10 Price or Fee Adjustment for Illegal or Improper Activity
52.203-12 Limitation on Payments to Influence Certain Federal Transactions
52.203-16 Preventing Personal Conflicts of Interest
52.203-17 Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights
52.204-13 System for Award Management Maintenance
52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
52.204-26 Covered Telecommunications Equipment or Services—Representation
52.204-27 Prohibition on a ByteDance Covered Application
52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment.
52.215-2 Audit and Records Negotiation
52.215-8 ORDER OF PRECEDENCE – UNIFORM CONTRACT FORMAT
52.215-23 LIMITATION ON PASS-THROUGH CHARGES

52.222-21 PROHIBITION OF SEGREGATED FACILITIES
52.222-26 EQUAL OPPORTUNITY
52.222-29 NOTIFICATION OF VISA DENIAL
52.222-50 COMBATING TRAFFICKING IN PERSONS
52.223-6 DRUG-FREE WORKPLACE
52.223-18 ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING
52.225-13 RESTRICTIONS ON CERTAIN FOREIGN PURCHASES
52.227-14 RIGHTS IN DATA – GENERAL
52.242-15 STOP-WORK ORDER
ALTERNATE I
52.243-2 CHANGES – COST-REIMBURSEMENT
ALTERNATE I (use 52.243-1 for fixed price)
52.243-3 Changes – Time-and-Material or Labor-Hours
52.244-2 SUBCONTRACTS
52.244-5 COMPETITION IN SUBCONTRACTING
52.244-6 SUBCONTRACTS FOR COMMERCIAL ITEMS
52.245-1 GOVERNMENT PROPERTY
52.246-3 INSPECTION OF SUPPLIES COST-REIMBURSEMENT
52.246-4 INSPECTION OF SERVICES FIXED-PRICE
52.246-5 INSPECTION OF SERVICES COST-REIMBURSEMENT
52.246-6 INSPECTION TIME-AND-MATERIAL AND LABOR-HOUR
52.246-25 LIMITATION OF LIABILITY – SERVICES
52.247-63 PREFERENCE FOR U.S. FLAG AIR CARRIERS
52.247-64 PREFERENCE FOR PRIVATELY OWNED U.S.-FLAG COMMERCIAL VESSELS
52.249-6 TERMINATION (COST REIMBURSEMENT)
52.253-1 COMPUTER GENERATED FORMS

AIDAR (https://www.usaid.gov/sites/default/files/2024-02/aidar_020524.pdf)
752.7013 Contractor-Mission Relationships (M/OAA-DEV-AIDAR-20-03c) Contractor-Mission Relationships
752.202-1(B) USAID DEFINITIONS CLAUSE – GENERAL SUPPLEMENT FOR US IN ALL USAID CONTRACTS (ALTERNATE 70)
752.202-1(D) USAID DEFINITIONS CLAUSE – SUPPLEMENT FOR USAID CONTRACTS INVOLVING PERFORMANCE OVERSEAS (ALTERNATE 72)
752.204-72 ACCESS TO USAID FACILITIES AND USAID'S INFORMATION SYSTEMS
752.209-71 Organizational Conflicts of Interest Discovered After Award
752.222-70 USAID Disability Policy
752.225-70 Source and Nationality Requirements
752.228-70 Medical Evacuation (MEDEVAC) Services
752.229-71 Reporting of Foreign Taxes
752.7027 PERSONNEL
752.7031 LEAVE AND HOLIDAYS
752.7032 International Travel Approval and Notification Requirements
752.7033 PHYSICAL FITNESS
752.7034 ACKNOWLEDGEMENT AND DISCLAIMER
752.7037 CHILD SAFEGUARDING STANDARDS
752.7038 NONDISCRIMINATION AGAINST END-USERS OF SUPPLIES AND SERVICES
752.7101 Voluntary Population Planning Activities

ANNEX H – Quick Start Guide for Getting a Unique Entity ID (UEI)

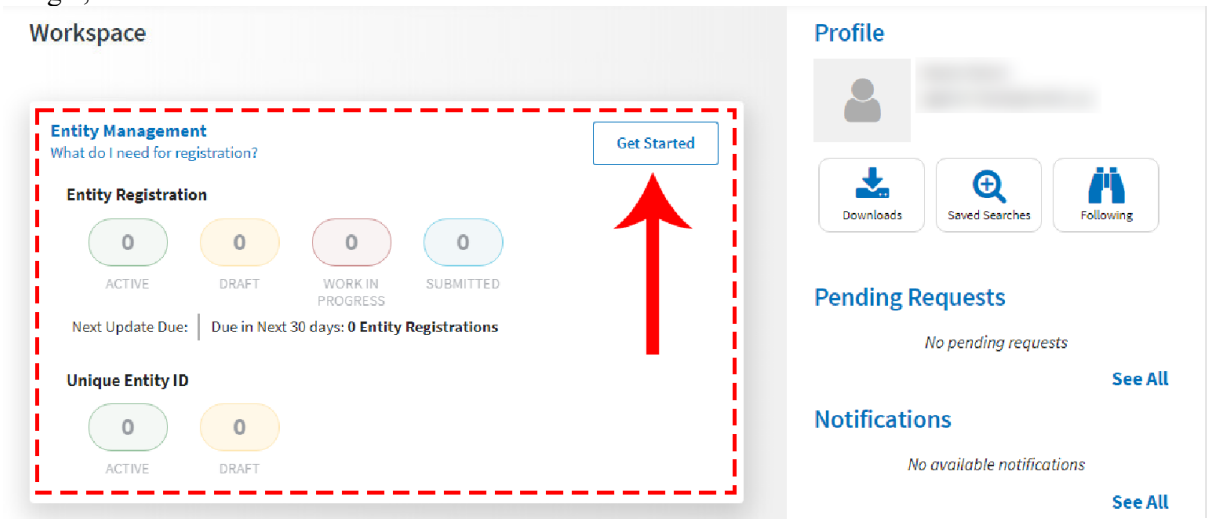
You can get a Unique Entity ID (UEI) for your organization without having to complete a full entity registration. If you only conduct certain types of transactions, such as reporting as a sub-awardee, you may not need to complete an entity registration. Your entity may only need a Unique Entity ID (UEI).

If you want to only get a Unique Entity ID (UEI and do not want to complete a full entity registration in SAM.gov, choose one of the following sections that best describes your entity:

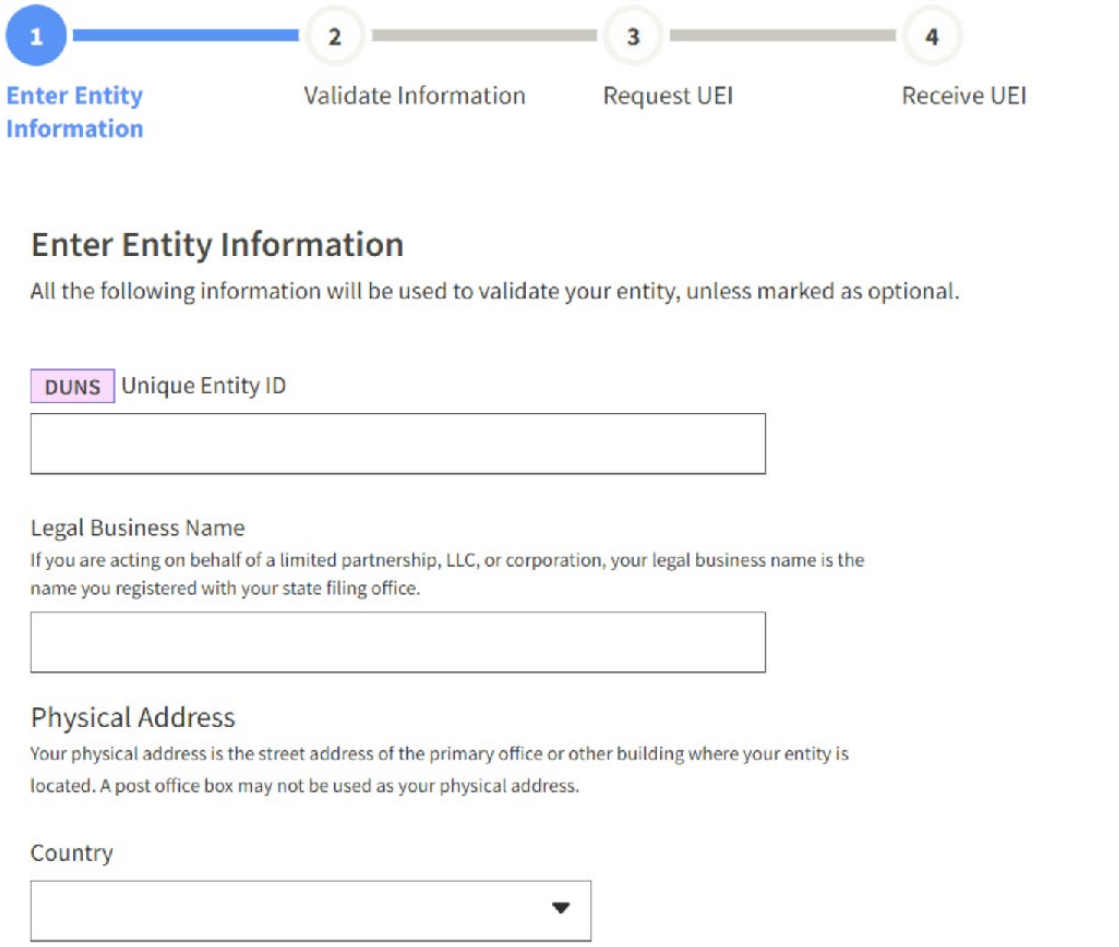
Your entity has a DUNS Number and is registered in SAM.gov
If you have an active or inactive registration in SAM.gov today, you've already been assigned a Unique Entity ID (UEI). It's viewable on your entity registration record in SAM.gov. Learn how to view your Unique Entity ID (UEI) here.

Your entity has a DUNS Number and is <u>not</u> registered in SAM.gov
If you currently have a DUNS Number, only need to get a Unique Entity ID (UEI), and do not want to complete a full entity registration in SAM.gov, follow these steps to get a Unique Entity ID (UEI):

1. Go to SAM.gov and select "Sign In" from the upper right corner of the page. If you do not have a SAM.gov account, you will need to create one. SAM.gov uses Login.gov for authentication. Once you create your user credentials, you will return to SAM.gov to complete your profile.
2. After you sign in, the system will navigate you to your Workspace. On the "Entity Management" widget, select the "Get Started" button.

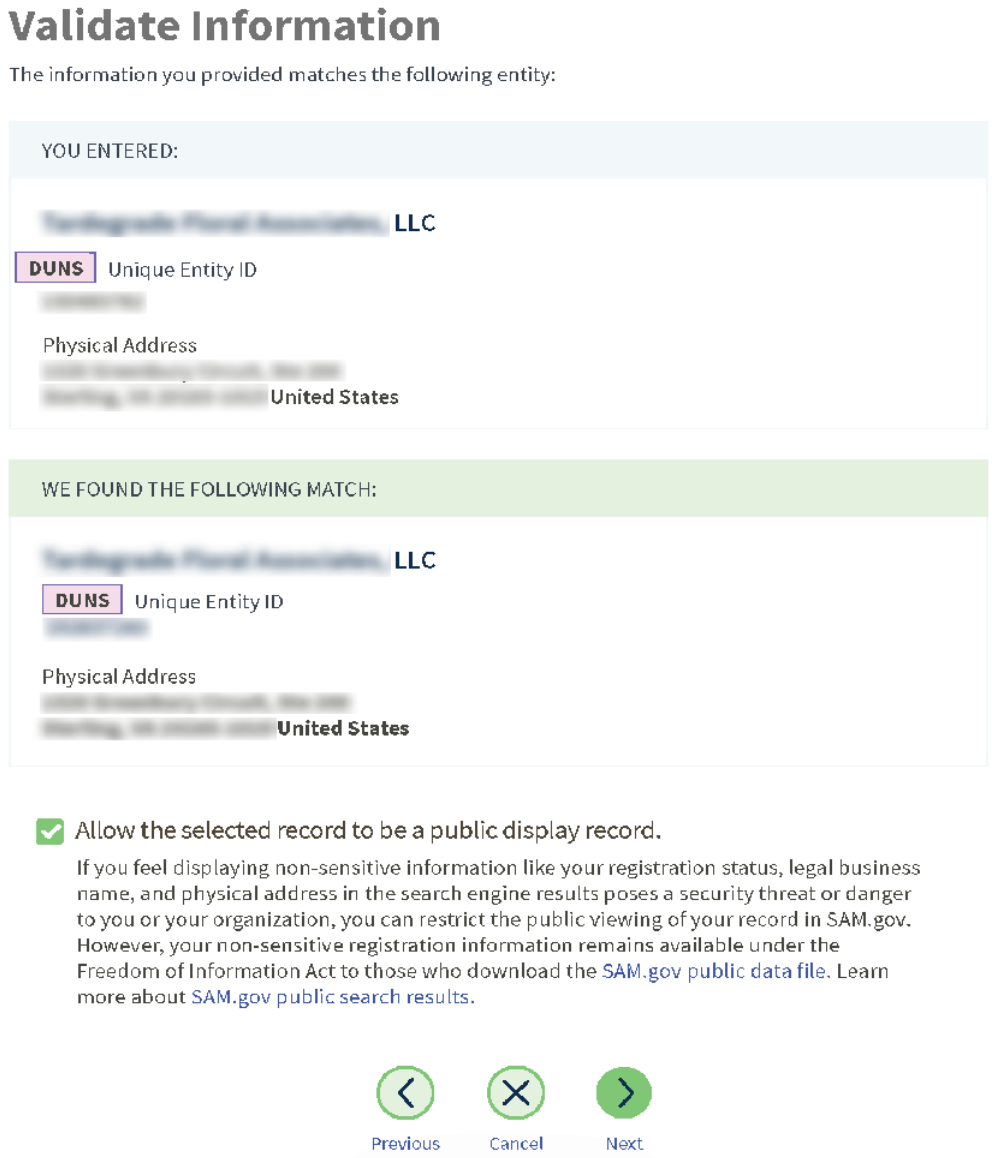


3. On the next page, enter information about your entity. All fields are required, unless marked as optional.

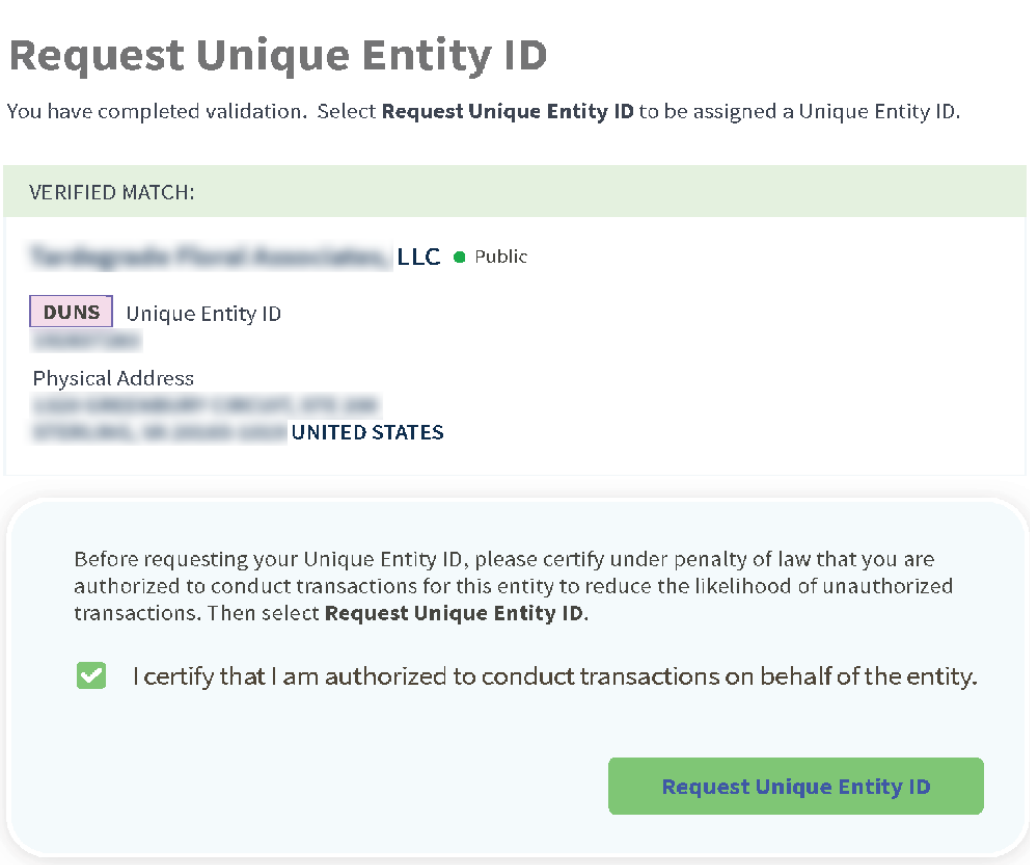


4. On the next page, validate that the information provided is correct. If the information provided does not match your Dun & Bradstreet record exactly, you will be able to proceed. For assistance updating your Dun & Bradstreet record, please contact Dun & Bradstreet.

   Deselect the checkbox near the bottom of the page if you want to restrict the public viewing of your entity information in SAM.gov. If you deselect the checkbox, only you and federal government users will be able to view your Unique Entity ID (UEI). Other entities and users of SAM.gov will not be able to view your Unique Entity ID (UEI) . Then, select “Next.”



5. On the next page, your entity is validated. You will be asked to certify that you are authorized to conduct transactions on behalf of your entity. Select the checkbox to certify, then select the "Request Unique Entity ID" button.



6. On the last page, your Unique Entity ID (UEI) will be displayed, and you can begin to use it for your entity.

As of April 4, 2022, the federal government will have no requirement for the DUNS Number. You can get a Unique Entity ID (UEI) for your entity on SAM.gov. The Unique Entity ID (UEI) is provided to entities who request to only get a Unique Entity ID (UEI) and to entities who complete an entity registration.

Sign in to your SAM.gov account and the system will navigate you to your Workspace. On the “Entity Management” widget, select the “Get Started” button to begin requesting your Unique Entity ID (UEI).