NATHAN

Trusted for Excellence

REQUEST FOR PROPOSAL (RFP)

No. RFP-IGNITE-JKT-22-0001

TO: Potential Bidders

FROM: Caroline Rubin, Chief of Party
ASEAN-USAID IGNITE Project
Contract No. 72049718C00004

ISSUANCE DATE: 23 February 2022 (GMT+7)

DEADLINE FOR RECEIPT OF QUESTIONS: 4 March 2022, 5:00 PM (GMT+7)

SUBMISSION DATE: 23 March 2022, 5:000 PM (GMT+7)

RE: **Development of E-Learning Content on Business Continuity and Resilience for ASEAN SMEs COVID-19 Recovery and Transformation**

Nathan Associates Inc. (Nathan Associates), as prime contractor of the U.S. Agency for International Development-funded project ASEAN-USAID IGNITE Project is seeking technical and price proposals from eligible firms to deliver the COVID-19 Tab e-learning content (self-paced e-learning modules, webinars, communities of practice, curated tools and resources, and other innovative learning approaches) on business continuity and resilience to equip and support ASEAN SMEs in their COVID-19 recovery and transformation.

Nathan Associates intends to award a **firm fixed price** contract for this activity with an estimated start date of 25 April 2022. The total estimated value of this RFP is USD 125,000 – USD 140,000, which is subject to availability of funds. Offerors are encouraged to outline cost-effective approaches, including using public-private alliances, which will achieve project objectives.

This RFP is open to qualified companies as defined in the technical instructions (note the geographic limitation).

All potential offerors are also informed that the contractor that is awarded a contract issued pursuant to this RFP will not be eligible to participate in any subsequent RFPs that involves evaluation of work done under this RFP, or any other activity that may result in conflict of interest because of the work performed under this RFP.

Technical and price proposal requirements, as well as proposal evaluation criteria, are outlined in **Annex A**. Nathan Associates intends to make a contract award to the responsible Offeror(s) whose proposal(s) represent the best value to the U.S. government.

Proposals are due in electronic copy only, in MS Word, MS Excel, and/or PDF formats, by 23 March 2022 (GMT+7). 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 ASEAN.USAID.IGNITE.programs@gmail.com.

Price proposals should include filled out and signed documentation attached in **annexes B, C and D**. All offerors should also review information included in **annex E** (relevant regulations).

Questions regarding this RFP are due in electronic copy by 4 March 2022, 5:00 PM, (GMT+7). They must be emailed (no phone questions will be accepted) to ASEAN.USAID.IGNITE.programs@gmail.com. Potential bidders who do not submit questions should 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 Nathan Associates to award a contract nor does it commit Nathan Associates to pay for any costs incurred in the preparation and submission of a proposal in response hereto. Furthermore, Nathan Associates reserves the right to reject any and all offers, if such action is considered to be in the best interest of USAID.

Sincerely,

Caroline Rubin, Chief of Party
ASEAN-USAID IGNITE Project

CONTENTS

TECHNICAL INSTRUCTIONS

Development of E-Learning Content on Business Continuity and Resilience for ASEAN SMEs COVID-19 Recovery and Transformation

Approx. Start Date:	18 April 2022
Approx. End Date:	Deliverables to be completed by September 2022; six-month maintenance period to begin after that30 September 2022

ACTIVITY BACKGROUND

The ASEAN SME Academy, an e-learning platform developed six years ago through collaborative effort between USAID, the U.S.-ASEAN Business Council (U.S.-ABC) and the ASEAN Coordinating Committee on Micro, Small and Medium Enterprises (ACCMSME). The core of the Academy is a series of courses for SMEs from member companies of US-ABC. In 2021, the Academy began a revamp process to improve overall user experience and accessibility of the website.

One of the new features in the revamped website (hereinafter "Academy 2.0") is the COVID-19 Tab, which will be led by the ASEAN-USAID Inclusive Growth in ASEAN through Innovation, Trade, and E-Commerce (ASEAN-USAID IGNITE) project, implemented by Nathan Associates Inc. The COVID-19 Tab is envisioned to be a one stop webpage where ASEAN SME Academy users can access e-learning modules, webinars, communities of practice, and curated tools and resources on business continuity and resilience to equip and support them in their COVID-19 economic recovery and transformation.

Business continuity is defined by ISO 22300:2018 standard as "*the capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruption*". The COVID-19 Tab will provide content[1] for ASEAN SMEs on how to anticipate disruptions (i.e., natural disasters or pandemics) and prepare a plan to ensure that business operations can continue if disruptions materialize.

Business resiliency is defined by ISO 2231:2017 standard as "*the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper.*" The COVID-19 Tab will provide content for SMEs to learn how to develop and enact mechanisms that enable them to adapt to sudden or incremental changing conditions and continue business operations.

The topics within business continuity and business resiliency will be based on the most pressing needs of SMEs in the ASEAN region and will be identified through a learning needs assessment. The content will not attempt to cover all aspects of business continuity and resilience, but rather respond to the current and most pressing needs of SMEs in the

[1] COVID-19 Tab (minimum) content consist of: E-Learning Modules, Webinars, Communities of practice, and curated tools and resources. Other proposed innovative learning approaches are welcome.

region. This will offer an opportunity for other partners to add content in the future that is perceived as important additional components of business continuity and resilience.

Business continuity and resilience are not new concepts, and several organizations such as the International Labor Organization (ILO), the United Nations Office for Disaster Risk Reduction (UNDRR), the Washington Small Business Development Center (SBDC), and U.S.-ABC member companies such as Facebook and UPS have developed booklets, checklists, and guidebooks on the topic. The COVID-19 Tab is not intended to reinvent the wheel but to create modules that are evidence-based and draw upon the best available resources and tailor them to various digital learning content that will cater to the need and characteristics of ASEAN SMEs.

OBJECTIVES OF THE ACTIVITY

The ASEAN-USAID IGNITE project, to engage a consultant/firm to deliver the COVID-19 Tab e-learning content (self-paced e-learning modules, webinars, communities of practice, curated tools and resources, and other innovative learning approaches) on business continuity and resilience to equip and support ASEAN SMEs in their COVID-19 recovery and transformation.

The COVID-19 Tab is envisioned to have, at minimum:

- 2 modules each for business continuity and business resilience (4 total modules);
- 4 self-paced courses per module (16 total courses);
- 2 webinars per module (8 total webinars);
- 4 guided discussions/communities of practice per module (16 total guided discussions/communities of practice); and
- Curated tools for business continuity and business resilience.

The content (self-paced e-learning modules, webinars, communities of practice, curated tools and resources (and other innovative learning approaches) are to be made available in four languages: English, Bahasa Indonesia, Thai, and Vietnamese. The courses should be completed in four languages, and the webinars can be subtitle/direct translations in the three languages.

The two business continuity modules will be launched by July 2022 and the two business resilience modules will be launched by August 2022.

QUALIFICATION AND EXPERIENCE OF CONTRACTOR

The contractor must have a good track record in terms of successful project(s) of similar nature in the area of:

- The consultant firm's team must be comprised of qualified experts, with a demonstrated track record in developing high quality e-learning materials for SMEs especially in business continuity and business resilience;
- It is expected that the team have experience developing high quality e-learning using experience developing high quality e-learning using online learning management systems, such as Thinkific, Moodle, Adobe Captivate, with preference for experience on Thinkific (on Magento platform);
- The team should have knowledge and experience of delivering e-learning in developing countries, particularly in Southeast Asia;
- The firm should have a strong project management ability and excellent communication skills;

- Examples of past work are required and should be included in the proposal;
- Analytical and conceptual skills;
- Ability to work against deadlines and in GMT+7 time zone.

Team composition (at minimum):

- A project manager who is an expert on e-learning design
- Technical Experts in Business Continuity and Business Resilience (or two technical experts)
- Graphic Designer (to produce the graphic for the self-paced courses), and
- Thinkific expert

SCOPE OF WORK AND DELIVERABLES

The Contractor shall submit the following deliverables:

No.	Activities	Deliverables	Illustrative Timeframe
1.	Completion of learning need assessment and instructional strategy	• Inception Report with outcomes of learning needs analysis, recommendations and work plan for the overall assignment. • The instructional strategy along with storyboards (and structure) for the modules, webinars, communities of practice, etc. • Review and sign-off by IGNITE on the instructional strategy with consultation with partners (US-ABC and DTI/PTTC)	3 weeks 2 weeks
2.	Production of the Business Continuity modules	• Production	4 weeks
3.	Functional Prototype Delivery	• The draft version of complete functional modules for Business Continuity ready for trial and feedback from partners and IGNITE. • Facilitate pilot testing for IGNITE and partners to test the modules and amend it according to IGNITE and partners' feedback. • Feedback from IGNITE and stakeholders addressed • Sign-off by IGNITE on the functional prototype.	Estimated date: 2nd week of June 2022 1 week 1 week
4.	Delivery of Completed Functional Module	• Delivery of the final version of the two modules on Business Continuity and its setup in the ASEAN SME Academy LMS – **Thinkific**	2 weeks
5.	Testing the modules on the ASEAN SME Academy	• Facilitate testing for IGNITE and partners to test the e-learning • Provide any needed fixes, fine-	1 week 1 week

		tunings and configurations based on the pilot testing. • Pilot testing report submitted	
6.	Business Continuity Modules go live	Content is live	Estimated date: July 2022
7.	Business Resilience Modules go live	Content is live	Estimated date: August 2022
8.	Submit operational manual in English and provide a mini-workshop for PTTC-DTI and US-ABC on the course Thinkific administration.	• Submit operational manual in English. • Provide training to IGNITE and partners on how to use the e-learning content.	Estimated date: September 2022 2 weeks 1 week
9.	After Launch	• Provide support if errors arise in any of the four modules after the final launch and acceptance of the e-learning tool for 6 months.	6 months

PAYMENT STRUCTURE

This will be a Firm Fixed Price contract. The subcontractor will be paid within thirty (30) calendar days after receipt of a proper invoice and acceptance of deliverables and in accordance with the payment schedule of the awarded contract.

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 Contractor within thirty (30) calendars 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, 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.

DURATION

The deliverables should be completed between 18 April 2022 through 30 September 2022. The six-month maintenance support period will follow.

WARRANTY

If applicable, the Contractor shall be required to provide the license(s) of 3rd party software, if any, during the duration of the project until the end of the agreed operational period.

The Contractor shall provide maintenance services in support of the software license during the life of this contract. Maintenance services shall cover technical support services that include error corrections, enhancement of capabilities, and optimization.

PROJECT MONITORING AND REPORTING

The Contractor shall propose the appropriate approach 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 to Galuh Wulan, Program Manager Digital Economy every week to monitor the progress of the project (including reports mentioned in the scope of work and deliverables).

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 Nathan Associates and Nathan Associates' 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 Nathan Associates 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.

ANNEX A – Technical and Price Proposal Requirements and Proposal Evaluation Criteria

Proposals are due in electronic copy only, in MS Word, MS Excel, and/or PDF formats, by 23 March 2022 (GMT+7). 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 ASEAN.USAID.IGNITE.programs@gmail.com.

Technical proposals shall consist of no more than twenty (20) pages and include details of the approach, timelines for completion of the project, a summary of qualifications of key personnel who would be assigned to the project, and necessary contact information. Additional tables, technical instructions, and CVs of key personnel, not to exceed two pages in length each, should be included in an appendix to the technical proposal and will not count towards the 20-page limit (margins should be 1 inch on each side, text should be single spaced, and font should be no less than 11 point). A separate financial proposal shall be provided. No cost information shall be provided in the technical proposal. Detailed specifications of the technical and financial proposals are shown below.

Your proposal shall be accompanied by a letter of transmittal prepared on your company letterhead stationery and signed by an individual authorized to commit the company to the proposal. The cover letter shall identify the following as well as all enclosures being transmitted as part of the proposal:

- The name, and address, of your company
- RFP number
- Point of Contact name, title, telephone number and email address
- Sam Unique Entity Identifier (UEI)
- Acknowledgement that it transmits an offer in response to the RFP that is valid for a minimum of 60 days from the proposal due date.

A. Technical Approach

The offeror shall prepare an innovative technical approach describing how it proposes to address the tasks outlined in the Technical Instructions. The technical approach shall show at least: i) an understanding of the work to be done and ii) a description of how the work will be organized, prioritized, and accomplished.

B. Work Schedule

The offeror shall prepare a work schedule for tasks laid out in the technical instructions. The work schedule shall include a short description of the major activities, realistic timeframes for accomplishing each major activity, personnel that will be needed to accomplish each major task, and level of effort (person days/person hours) needed for each person listed. This work schedule shall be provided in table format in MS Word or MS Excel and include the full period of performance.

C. Project Management

The offeror shall propose the appropriate approach for project monitoring and reporting processes that will meet the project objectives. In its approach the offeror shall cover at minimum the following elements:

- The offeror shall briefly describe how the project will be managed and by whom, reporting relationships, etc.
- The offeror shall propose the project team structure and the relationships between the various functions of the structure, accompanied by a description of each function.
- The offeror may choose to propose the project management methodology, project coordination, organizational structure, contract management, quality assurance, resource management, and its approach to sustainability.
- The offeror should include any assumptions made.
- In addition, the offeror may identify the resources, roles responsibilities and skills needed to execute the activities and tasks identified.

D. Firm and Personnel Qualifications and Past Performance

The offeror must be a firm and must demonstrate a good track record in conducting successful activities and projects of similar nature, notably in the area of e-learning on business continuity and resilience for SMEs.

1. The offeror must be able to access competent experts with experience in relevant areas such as:
    a. Design and delivery of innovative and engaging e-learnings for SMEs
    b. Subject matter expert in Business Continuity and Business Resilience
    c. Experience working in Southeast Asia especially with SMEs
    d. Design and setup of the courses in Thinkific - LMS on Magento platform
    e. Design aesthetic
    f. Translation for Bahasa Indonesia, Thai and Vietnamese
2. The offeror shall include the company background and capability to carry out the work and relevant experience in conducting similar work. Background to be provided by the offeror shall include:
    a. Academic qualifications
    b. Summary of previous work completed that is of similar or related nature to the one described in the technical instructions
    c. Sample(s) of work completed, including design aesthetic
    d. Composition of the expert team and CVs of key personnel

The offeror shall also attach three (3) specific references with name and telephone numbers of clients that have contracted offeror's services for work that is similar or related to the one requested in this solicitation in the last two years.

E. Price Proposal

Offerors are required to submit a detailed price proposal, which needs to include a table (in MS Excel) showing a breakdown of cost per deliverable (and sub-deliverable) outlined in the Tasks and Deliverables section of the technical instructions. The cost breakdown needs to

include total cost per deliverable/sub-deliverable. Please provide a firm-fixed price value for each deliverable. These values will be established as a payment schedule and paid within 30 days after acceptable invoice to include approved deliverable. The price proposal should be submitted in a separate file and should not be included as part of the technical offer.

F. Additional Requirements

In accordance with FAR Subpart 9.5 please complete and sign the OCI Certification Form which certifies if your organization has any actual or potential OCI concerns. An OCI plan is not required if there are no current or potential OCI concerns.

Please confirm you have a SAM UEI or are in the process of obtaining one. See **Annex F** for instructions.

Please include a completed Evidence of Responsibility Form found in Annex D.

G. Evaluation Criteria

The following table includes the components for both technical and cost evaluations. The total points for a perfect scoring have been included. The evaluation panel will use these weights for evaluating the proposals. The offeror proposing the best overall value for money will be selected. Offerors' proposals need to cover all items listed in the Table below, preferably in the same order presented. No additional information other than what is requested in this Annex A and the Table below will be evaluated.

Criterion	**Maximum Points**	**Score**
Technical approach	40	
Work schedule (including level of effort, key personnel for each major task, and timeframe)	15	
Project management structure	15	
Firm qualifications and Past Performance	30	
Total points	**100**	

Cost will be evaluated separately.

H. Estimated Award Timeline

Activity	**Estimated Dates**
- Request for proposals issued	23 February 2022
- Deadline to submit questions	4 March 2022
- Deadline to submit offers	23 March 2022
- Award made (after evaluations, reference checks, and USAID approval)	18 April 2022
- Expected start date	25 April 2022
- Expected completion date	30 September 2022

I. Language of Submissions

The offers and all deliverables shall be submitted in the English language. All input and material received by the Consultant in the course of conducting the work shall be provided to the ASEAN-USAID IGNITE Project either in the original language or, if translation was performed, in English.

J. Submission Information

The technical and price proposals must be submitted electronically in separate files. Offerors may send their technical offers in MS Word or PDF files. Each email must not exceed 5MB in size. Cost offers should be in MS Word or PDF files with MS Excel files for all tables. Table attachments to the technical proposal in MS Excel may be used where necessary. Electronic versions must be sent to the addressees listed in the cover letter. The offerors are responsible for ensuring that the proposal is received in due form by the deadline provided in the cover letter.

(a) Nathan Associates may award a contract without discussions with Offerors in accordance with FAR 52.215-1.

(b) Nathan Associates intends to evaluate Offerors in accordance with **Annex A** of this RFP and make contract award to the responsible Offeror whose proposal represents the best value to the U.S. Government. "Best value" is defined as the offer that results in the most advantageous solution for the Government, in consideration of technical, cost, and other factors. For evaluation purposes, technical factors are considered more important than cost factors. Although technical evaluation criteria are more important than cost, the closer the technical evaluation scores of the various proposals are to one another, the more important cost considerations will become. Therefore, the evaluation of costs proposed may become a determining factor in making the award as technical scores converge. The Offeror proposing the best overall value will be selected. Any lack of cost realism, reasonableness, incompleteness, or imbalance in price may be considered in the determination of best value.

(c) Nathan Associates may request additional certifications, clarification and explanations in order to determine the best value proposal.

ANNEX B – Representations, Certifications and Other Statements of Offerors

NATHAN ASSOCIATES INC.
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	
DUNS NUMBER (FAR 52.204-6)	
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/regulatio	Enter the 6-digit NAICS Code that most closely represents the product, commodity or service that your firm is likely to sell to Nathan Associates Inc. in the calendar year covered by these representations. NAICS Code:

Company Information	
Approved accounting system	☐ Yes ☐ No
If so, last review date: Click here to enter text.	If so, name the reviewing agency: Click here to enter text.
Approved estimating system	☐ Yes ☐ No
If so, last review date: Click here to enter text.	If so, name the reviewing agency: Click here to enter text.
Approved purchasing system (FAR part 44)	☐ Yes ☐ No
If so, last review date: Click here to enter text.	If so, name the reviewing agency: Click here to enter text.
Approved government property system? (FAR part 45)	☐ Yes ☐ No
If so, last review date: Click here to enter text.	If so, name the reviewing agency: Click here to enter text.
Approved Earned Value Management System?	☐ Yes ☐ No
If so, last review date: Click here to enter text.	If so, name the reviewing agency: Click here to enter text.

Annual Incurred Cost data submitted in accordance with 6 month deadline after fiscal year closeout?	☐ Yes ☐ No Enter last calendar year completed
Last year negotiated Indirect rate agreement approved completed in accordance with 6 month deadline?	☐ Yes ☐ No Enter last calendar year completed
Last year closeout completed in accordance with 6 month deadline?	☐ Yes ☐ No Enter last calendar year completed

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 Associates Inc. Procurement Compliance Office.

TYPE OF BUSINESS ORGANIZATION (MUST BE ON FILE FOR EACH SUPPLIER) – (FAR 52.204-3)

Taxpayer Identification Number (TIN) ☐ TIN:54-1670018,

☐ TIN has been applied for

☐ TIN is not required because:

☐) Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐ Offeror is an agency or instrumentality of a foreign government;

☐ Offeror is an agency or instrumentality of the Federal Government.

The offeror, by checking the applicable box, represents that it operates as-

☐) a corporation incorporated under the laws of the State of VA,

☐ a sole proprietorship

☐ a government entity (Federal, State, or local)

☐ a foreign entity and if a corporation registered for business in (country) (☐) a partnership

☐ an International organization per 26 CFR 1.6049-4 or ☐ a joint venture between

☐ an individual

☐ Offeror is not owned or controlled by a common parent as defined in paragraph (a) of this provision.

☐ Name and TIN of common parent:

Name

TIN

(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).

OFFEROR REPRESENTATIONS AND CERTIFICATIONS – COMMERCIAL ITEMS (FAR 52.212-3)

Buy American Act Certificate. (FAR 52.225-2) (Applies only if the clause at FAR 52.225-1, Buy American Act – Supplies, is included)

1. The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. The terms "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American Act—Supplies."

2. Foreign End Products:

Line Item Number: Country of Origin
N/A
(List as necessary)

(End of Provision)

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

(End of Provision)

PREVIOUS CONTRACTS AND COMPLIANCE REPORTS (FAR 52-222.22) (Feb 1999) – $10,000

a. OFFEROR ☐ has, ☐ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation;

b. OFFEROR ☐ has, ☐ has not, filed all required compliance reports and

c. Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

(End of Provision)

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—

(1) Exceeds $30,000 in value; and
(2) 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.

(i) *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 C – 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: http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm .

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 D – Evidence of Responsibility

COMPANY LETTERHEAD

Prime Contract # 72049718C00004
ASEAN-USAID Inclusive Growth in ASEAN through Innovation, Trade, and E-Commerce (ASEAN-USAID IGNITE)

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. Type of business/institution

Subcontractor certifies that it is a (indicate with "X" all that apply):

	Non-U.S. owned/operated		Service-disabled veteran-owned small business
	Non-profit		HUBZone small business
	Large/Other than small business		Small disadvantaged business
	Small business		Woman-owned small business
	Veteran-owned small business		

10. Subcontractor's DUNS and Employer Tax ID Numbers

Subcontractor's DUNS Number: Click here to enter DUNS 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 E – Relevant Regulations

Flow Down Clauses from Prime Contract

AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for this activity is "937". In general, local procurement is authorized subject to the provisions of AIDAR 752.225-71. Information on geographic codes can be found at http://www.usaid.gov/sites/default/files/documents/1876/310.pdf . Geographic Code 937 is defined as the United States, the cooperating country and developing countries other than advanced developing countries, and excluding prohibited sources. All ASEAN Member States are considered cooperating countries, except Singapore and Brunei.

LOGISTIC SUPPORT

The Contractor shall be responsible for furnishing all logistic support to fulfill the requirements of this assignment. These shall include all travel arrangements, appointment scheduling, secretarial services, report preparations services, printing, and duplicating.

EXECUTIVE ORDER ON TERRORISM FINANCING

The Offeror is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the contractor/recipient to ensure compliance with these Executive Orders and laws. This provision must be included in all subcontracts/subawards issued under this contract.

RESTRICTION ON ASSISTANCE TO ASEAN LAW ENFORCEMENT

Assistance may not be provided to police, prisons, or members of other law enforcement entities, unless a specific statutory exception is applicable. Members of "law enforcement entities" are generally those who have the authority to carry weapons, make arrests, interrogate in private, search private premises, or supervise confinement. Particular attention in this regard will be paid to activities involving anti-money laundering, counter-terrorism, and cyber crimes. Members of law enforcement entities will also be subject to Leahy Amendment vetting.

CONDOMS (ACQUISITION) (JUNE 2005)

Information provided about the use of condoms as part of projects or activities that are funded under this contract shall be medically accurate and shall include the public health benefits and failure rates of such use and shall be consistent with USAID's fact sheet entitled, "USAID:

HIV/STI Prevention and Condoms. This fact sheet may be accessed at: http://www.usaid.gov/our_work/global_health/aids/TechAreas/prevention/condomfactsheet.html

PROHIBITION ON THE PROMOTION OR ADVOCACY OF THE LEGALIZATION OR PRACTICE OF PROSTITUTION OR SEX TRAFFICKING (ACQUISITION) (APRIL 2010)

(a) This contract is authorized under the United States Leadership Against HIV/AIDS, Tuberculosis and Malaria Act of 2003 (P.L. 108-25). This Act enunciates that the U.S. Government is opposed to prostitution and related activities, which are inherently harmful and dehumanizing, and contribute to the phenomenon of trafficking in persons. The contractor shall not use any of the funds made available under this contract to promote or advocate the legalization or practice of prostitution or sex trafficking. Nothing in the preceding sentence shall be construed to preclude the provision to individuals of palliative care, treatment, or post-exposure pharmaceutical prophylaxis, and necessary pharmaceuticals and commodities, including test kits, condoms, and, when proven effective, microbicides.

(b) Except as provided in the second sentence of this paragraph, as a condition of entering into this contract or subcontract, a nongovernmental organization or public international organization contractor/subcontractor must have a policy explicitly opposing prostitution and sex trafficking. The following organizations are exempt from this paragraph: the Global Fund to Fight AIDS, Tuberculosis and Malaria; the World Health Organization; the International AIDS Vaccine Initiative; and any United Nations agency.

(c) The following definition applies for purposes of this provision: Sex trafficking means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act. 22 U.S.C.7102(9).

(d) The contractor shall insert this clause in all subcontracts.

(e) Any violation of this clause will result in the immediate termination of this contract by USAID." If the contract provides for the contractor to execute grants to nongovernmental organizations (not-for-profits or for-profits), per ADS 302.5.6 Grants under Contracts, then the contractor must comply with the assistance provisions in Section 3.A of this AAPD when awarding grants or cooperative agreements under its contract (in compliance with ADS 302.5.6(c) and (d)).

PROHIBITION ON THE USE OF FEDERAL FUNDS TO PROMOTE, SUPPORT, OR ADVOCATE THE LEGALIZATION OR PRACTICE OF PROSTITUTION – TIP (ACQUISITION) (MAY 2007)

(a) The U.S. Government is opposed to prostitution and related activities, which are inherently harmful and dehumanizing, and contribute to the phenomenon of trafficking in persons. None of the funds made available under this contract may be used to promote, support, or advocate the legalization or practice of prostitution. Nothing in the immediately preceding sentence shall be construed to preclude assistance designed to ameliorate the suffering of, or health risks to, victims while they are being trafficked or after they are out of the situation that resulted from such victims being trafficked.

(b) The contractor shall insert this clause, in its entirety, in all sub-awards under this award.

(c) This provision includes express terms and conditions of the contract and any violation of it shall be grounds for unilateral termination of the contract, in whole or in part, by USAID prior to the end of the term.

RIGHTS TO PROPOSAL DATA

It is agreed that as a condition of award of this contract, and notwithstanding the conditions of any notice appearing thereon, USAID and ASEAN USAID IGNITE shall have unlimited rights (as defined in the "Rights in Data--General" clause contained in this contract) to all information included in the proposals submitted and to the technical data contained in the proposal.

MEDEX/MEDEVAC SERVICES

AIDAR 752.228-70 Medical Evacuation (MEDEVAC) Services (July 2007) (Pursuant to class deviation OAA-DEV-2006-1c)

(a) Contractor must provide MEDEVAC service coverage to all U.S. citizen, U.S. resident alien, and Third Country National employees and their authorized dependents (hereinafter "individual") while overseas under a USAID-financed direct contract. USAID will reimburse reasonable, allowable, and allocable costs for MEDEVAC service coverage incurred under the contract. The Contracting Officer will determine the reasonableness, allowability, and allocability of the costs based on the applicable cost principles and in accordance with cost accounting standards.

(b)Exceptions.

(i) The Contractor is not required to provide MEDEVAC insurance to eligible employees and their dependents with a health program that includes sufficient MEDEVAC coverage as approved by the Contracting Officer.
(ii) The Mission Director may make a written determination to waive the requirement for such coverage. The determination must be based on findings that the quality of local medical services or

other circumstances obviate the need for such coverage for eligible employees and their dependents located at post.

(c) Contractor must insert a clause similar to this clause in all subcontracts that require performance by contractor employees overseas.

AIDAR 48 CFR CHAPTER 7 CLAUSES INCORPORATED BY REFERENCE

AIDAR 752.211-70 LANGUAGE AND MEASUREMENT JUN 1992

EXECUTIVE ORDER ON TERRORISM FINANCING (FEB 2002)

The Contractor/Recipient is reminded that U.S. Executive Orders and U.S. law prohibits transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. It is the legal responsibility of the Contractor to ensure compliance with these Executive Orders and laws. This provision must be included in all subcontracts/sub-awards issued under this contract.

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

(a) Definitions. As used in this contract -- "Information Technology" means

(1) Any services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency; where

(2) such services or equipment are ' used by an agency' if used by the agency directly or if used by a contractor under a contract with the agency that requires either use of the services or equipment or requires use of the services or equipment to a significant extent in the performance of a service or the furnishing of a product.

(3) The term " information technology" includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including provisioned services such as cloud computing and support services that support any point of the lifecycle of the equipment or service), and related resources.

(4) The term "information technology" does not include any equipment that is acquired by a contractor incidental to a contract that does not require use of the equipment. (OMB M-15-14)

(b) The Federal Information Technology Acquisition Reform Act (FITARA) requires Agency Chief Information Officer (CIO) review and approval of contracts or interagency agreements for information technology or information technology services.

(c) The approved information technology and/or information technology services are specified in the Schedule of this contract. The Contractor must not acquire additional information technology without the prior written approval of the Contracting Officer as specified in this clause.

(d) Request for Approval Requirements:

(1) If the Contractor determines that any information technology in addition to that information technology specified in the Schedule will be necessary to meet the Government's requirements or to facilitate activities in the Government's statement of work, the Contractor must request prior written approval from the Contracting Officer.

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

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

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

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

RESTRICTIONS AGAINST DISCLOSURE (MAY 2016)

(a) The Contractor agrees, in the performance of this contract, to keep the information furnished by the Government or acquired/developed by the Contractor in performance of the contract and designated by the CO or COR, 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 CO 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.

MEDIA AND INFORMATION HANDLING AND PROTECTION (APRIL2018)

(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;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 "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 FAR, Privacy Act of 1974 (5 U.S.C. 552a - the Act), E- Government Act of 2002 - Section 208 and Title III, FISMA, the 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).

PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEM INCIDENT REPORTING (APRIL 2018)

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

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

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

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (APRIL 2018)

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

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

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

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

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

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

(b) Applicability: This special contract requirement applies to the Contractor, its subcontractors, and all personnel providing support under this contract (hereafter referred to collectively as

"Contractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, FISMA, the HIPAA (Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), NIST, FIPS and the 800-Series Special Publications (SP), OMB memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.

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

(1) HSPD-12 Compliance

i. Procurements for services and products involving facility or system access control must be in accordance with HSPD-12 policy and the Federal Acquisition Regulation.

ii. All development for USAID systems must include requirements to enable the use Personal Identity Verification (PIV) credentials, in accordance with NIST FIPS 201, PIV of Federal Employees and Contractors, prior to being operational or updated.

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

(3) Secure Configurations

i. The Contractor's applications must meet all functional requirements and operate correctly as intended on systems using the United States Government Configuration Baseline (USGCB) or the current configuration baseline.

ii. The standard installation, operation, maintenance, updates, and/or patching of software

must not alter the configuration settings from the approved USGCB configuration. The information technology, when applicable, must also use the Windows Installer Service for installation to the default "program files" directory and must be able to silently install and uninstall.

iii. Applications designed for normal end users must run in the standard user context without elevated system administration privileges.

iv. The Contractor must apply due diligence at all times to ensure that the required level of security is always in place to protect USAID systems and information, such as using Defense Information Systems Agency Security Technical Implementation Guides (STIGs), common security configurations available from the National Institute of Standards and Technology's website at https://nvd.nist.gov/ncp/repository or USAID established configuration settings.

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

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

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

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

(6) Contractor System Oversight/Compliance

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

ii. The Contractors must afford USAID the level of physical or logical access to the

Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases to the extent required to support its security and privacy programs. This includes monitoring, inspection, investigation and audits to safeguard against threats and hazards to the integrity, availability and confidentiality of USAID data or information systems operated on behalf of USAID; and to preserve or retrieve evidence in the case of computer crimes.

iii. All Contractor systems must comply with Information Security Continuous Monitoring (ISCM) and Reporting as defined in a continuous monitoring plan, to include, but not limited to, both automated authenticated and unauthenticated scans of networks, operating systems, applications, and databases. The Contractor must provide a continuous monitoring plan in accordance with NIST standards, as well as scan results upon request or at a minimum monthly to the COR and Contracting Officer, in addition to the CIO at ITAuthorization@usaid.gov. Alternatively, the Contractor may allow USAID information security staff to run scans directly.

iv. The Contractors must comply with systems development and lifecycle management best practices and processes as defined by Bureau for Management, Office of The Chief Information Officer (M/CIO) USAID IT Project Governance standards and processes for approval of IT projects, for the acceptance of IT project deliverables, and for the project's progression through its life cycle.

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

i. For all information systems procured, developed, deployed, and/or operated on behalf of the US Government information by the provision of this contract, the Contractor must provide a system security assessment and authorization work plan, including project management information, to demonstrate that it complies or will comply with the FISMA and NIST requirements. The work plan must be approved by the COR, in consultation with the USAID M/CIO Information Assurance Division.

ii. Prior to deployment of all information systems that transmit, store or process Government information, the contractor must obtain an Authority to Operate (ATO) signed by a USAID Authorizing Official from the contracting officer or COR. The Contractor must adhere to current NIST guidance for SA&A activities and continuous monitoring activities thereafter.

iii. Prior to the SA&A, a Privacy Threshold Analysis (PTA) must be completed using the USAID Privacy Threshold Analysis Template. The completed PTA must be provided to the USAID Privacy Officer or designate to determine if a Privacy Impact Analysis (PIA) is required. If a determination is made that a PIA is required, it must be completed in accordance with the USAID PIA Template, which USAID will provide to the Contractor as necessary. All privacy requirements must be completed in coordination with the COR or other designated Government staff.

iv. Prior to the Agency security assessment, authorization and approval, the Contractor must coordinate with the COR and other Government personnel as required to complete the FIPS

199 Security categorization and to document the systems security control baseline.

v. All documentation must be prepared, stored, and managed in accordance with standards, templates and guidelines established by USAID M/CIO. The USAID M/CIO or designee must approve all SA&A requirements.

(vi) In information systems owned or operated by a contractor on behalf of an agency, or for information collected or maintained by or on behalf of the agency, an SA&A must be done independent of USAID, to include the selection of a Federal Risk and Authorization Management Program (FEDRAMP) approved independent Third Party Assessor (3PAO). See approved list of Assessors at https://www.fedramp.gov/ /. The Contractor must submit a signed SA&A package approved by the 3PAO to USAID at saacapackages@usaid.gov at least 60 calendar days prior to obtain the ATO for the IT system.

vii. USAID retains the right to deny or rescind the ATO for any system if it believes the package or system fails to meet the USAID security requirements. Moreover, USAID may or may not provide general or detailed guidance to the Contractor to improve the SA&A package or the overall security posture of the information system and may or may not require re-submission of the package upon completion of the modifications. USAID reserves the right to limit the number of resubmissions at its convenience and may determine a system's compliance to be insufficient at which time a final determination will be made to authorize or deny operation. USAID is the final authority on the compliance.

viii. The Contractor must submit SA&A packages to the CIO at least sixty (60) days prior to production or the expiration of the current ATO.

ix. Once the USAID Chief Information Security Officer or designee determines the risks, the Contractor must ensure that all Plan of Action and Milestones resulting from security assessments and continuous monitoring are remediated within a time frame commensurate with the level of risk as follows:

- High Risk = 30 calendar days;
- Moderate Risk = 60 calendar days; and
- Low Risk = 180 calendar days

(8) Federal Reporting Requirements: Contractors operating information systems on behalf of USAID must comply with FISMA reporting requirements. Monthly, quarterly and annual data collections will be coordinated by USAID. Data collections include but are not limited to, data feeds in a format consistent with OMB requirements. The Contractor must provide timely responses as requested by USAID and OMB.

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

CLOUD COMPUTING (APRIL 2018)

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

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

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

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

"Information Security Incident" means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
(2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

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

"Spillage" means a security incident that results in the transfer of classified or other sensitive or sensitive but unclassified information to an information system that is not accredited,(i.e., authorized) for the applicable security level of the data or information. "Cloud Service Provider" or CSP means a company or organization that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses, organizations or individuals.

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

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

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

(b) Applicability

This special contract requirement applies to the Contractor and all personnel providing support under this contract (hereafter referred to collectively as "Contractor") and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), 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 Government data unless specifically authorized by the terms of this contract issued hereunder.

(i) If authorized by the terms of this contract issued hereunder, any access to, or use or disclosure of, Government data 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 Government data only to manage the operational environment that supports the government data 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, National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Contracting Officer all Government data and Government-related data, 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, e-Records and legal or security investigations.

(3) The Contractor shall retain and maintain all Government data 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 Government data and Government-related data 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 Government data: The Contractor shall notify the Government immediately of any requests from a third party for access to Government data or Government-related data, 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 Government data to a third party. The Contractor shall cooperate with the Government to take all measures to protect Government data 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: CSP must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect 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.

H.1 SUBMISSION TO THE DEVELOPMENT DATA LIBRARY (DDL)

Please refer to ADS 302, USAID Direct Contracting, Section 302.3.5.22, "Submission of Datasets to the Development Data Library (DDL)" for additional guidance.

a) Definitions – For the purpose of submissions to the DDL:

1) "Dataset" is an organized collection of structured data, including data contained in spreadsheets, whether presented in tabular or non-tabular form. For example, a Dataset may represent a single spreadsheet, an extensible mark-up language (XML) file, a geospatial data file, or an organized collection of these. This requirement does not apply to aggregated performance reporting data that the contractor submits directly to a USAID portfolio management system or to unstructured data, such as email messages, PDF files, PowerPoint presentations, word processing documents, photos and graphic images, audio files, collaboration software, and instant messages. Neither does the requirement apply to the contractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information. Datasets submitted to the DDL will generally be those generated with USAID resources and created in support of Intellectual Work that is uploaded to the Development Experience Clearinghouse (DEC) (see AIDAR 752.7005 "Submission Requirements for Development Experience Documents").

2) "Intellectual Work" includes all works that document the implementation, monitoring, evaluation, and results of international development assistance activities developed or acquired under this award, which may include program and communications materials, evaluations and assessments, information products, research and technical reports, progress and performance reports required under this award (excluding administrative financial information), and other reports, articles and papers prepared by the contractor under the award, whether published or not. The term does not include the contractor's information that is incidental to award administration, such as financial, administrative, cost or pricing, or management information.

b) Submissions to the Development Data Library (DDL)

1) The Contractor must submit to the Development Data Library (DDL), at www.usaid.gov/data, in a machine-readable, non-proprietary format, a copy of any Dataset created or obtained in performance of this award, including Datasets produced by a subcontractor at any tier. The submissions must include supporting documents describing the Dataset, such as code books, data dictionaries, data gathering tools, notes on data quality and explanations of redactions.

2) Unless otherwise directed by the CO or the COR, the contractor must submit the Dataset and supporting documentation within thirty (30) calendar days after the Dataset is first used to produce an Intellectual Work or is of sufficient quality to produce an Intellectual Work. Within thirty (30) calendar days after award completion, the Contractor must submit to the DDL any

Datasets and supporting documentation that have not previously been submitted to the DDL, along with an index of all Datasets and Intellectual Work created or obtained under the award. The Contractor must also provide to the COR an itemized list of any and all DDL submissions.

The Contractor is not required to submit the data to the DDL, when, in accordance with the terms and conditions of this award, Datasets containing results of federally funded scientific research are submitted to a publicly accessible research database. However, the Contractor must submit a notice to the DDL by following the instructions at www.usaid.gov/data, with a copy to the COR, providing details on where and how to access the data. The direct results of federally funded scientific research must be reported no later than when the data are ready to be submitted to a peer-reviewed journal for publication, or no later than five calendar days prior to the conclusion of the award, whichever occurs earlier.

3) The Contractor must submit the Datasets following the submission instructions and acceptable formats found at www.usaid.gov/data.

4) The Contractor must ensure that any Dataset submitted to the DDL does not contain any proprietary or personally identifiable information, such as social security numbers, home addresses, and dates of birth. Such information must be removed prior to submission.

5) The Contractor must not submit classified data to the DDL.

FAR 52.222-35 EQUAL OPPORTUNITY FOR VETERANS (OCT 2015)

(a) *Definitions*. As used in this clause--
"Active duty wartime or campaign badge veteran," "Armed Forces service medal veteran," "disabled veteran," "protected veteran," "qualified disabled veteran,' and "recently separated veteran" have the meanings given at FAR 22.1301.
(b) *Equal opportunity clause*. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.
(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $150,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate of identify properly the parties and their undertakings.
[Class Deviation- 2017-O0008, Office of Federal contract Compliance Programs Waiver of Certain Clause Requirements in Contracts for Hurricane Harvey Relief Efforts. This clause deviation is effective on Sept 01, 2017, and remains in effect until incorporated into the FAR, or otherwise rescinded.

(d) Notwithstanding the provisions of this section, the Contractor will not be obligated to develop the written affirmative action program required under the regulations implementing the Vietnam Era Veterans' Readjustment Assistance Act (VEVRAA).

FAR 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)

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

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

[Class Deviation- 2017-O0008, Office of Federal contract Compliance Programs Waiver of Certain Clause Requirements in Contracts for Hurricane Harvey Relief Efforts. This clause deviation is effective on Sept 01, 2017, and remains in effect until incorporated into the FAR, or otherwise rescinded.

(c)Notwithstanding the provisions of this section, the Contractor will not be obligated to develop the written affirmative action program required under the regulations implementing section 503 of the Rehabilitation Act of 1973, as amended.

AIDAR 752.228-3 WORKER'S COMPENSATION INSURANCE (DEFENSE BASE ACT) (DEC 1991)

As prescribed in AIDAR 728.309, the following supplemental coverage is to be added to the clause specified in FAR 52.228-3 by the USAID contracting officer. (See FAR 52.228)

(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.

(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 04/22/2016 Partial Revision 96 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 a like requirement to provide overseas workmen's compensation insurance coverage and obtain DBA coverage under the USAID requirements contract.

AIDAR 752.229-71 REPORTING OF FOREIGN TAXES (JULY 2007)

(a) The Contractor must annually submit a report by April 16 of the next year.
(b) Contents of Report. The reports must contain:
    a. Contractor name.
    b. Contact name with phone, fax number and e-mail address.
    c. Contract number(s).
    d. Amount of foreign taxes assessed by a foreign government [each foreign government must be listed separately] on commodity purchase transactions valued at
    $500 or more financed with U.S. foreign assistance funds under this agreement during the prior U.S. fiscal year.
    e. Only foreign taxes assessed by the foreign government in the country receiving
    U.S. assistance are to be reported. Foreign taxes by a third party foreign government are not to be reported. For example, if a contractor performing in Lesotho using foreign assistance funds should purchase commodities in South Africa, any taxes imposed by South Africa would not be reported in the report for Lesotho (or South Africa).
    f. Any reimbursements received by the Contractor during the period in paragraph
    (b) (4) of this clause regardless of when the foreign tax was assessed and any
    reimbursements on the taxes reported in paragraph (b)(4) of this clause received through March 31.
    g. Report is required even if the Contractor did not pay any taxes during the reporting period.
    h. Cumulative reports may be provided if the Contractor is implementing more than one program in a foreign country.
(c) Definitions. As used in this clause --
    (1) "Agreement" includes USAID direct and country contracts, grants, cooperative agreements and interagency agreements.
    (2) "Commodity" means any material, article, supply, goods, or equipment.
    (3) "Foreign government" includes any foreign governmental entity.
    (4) "Foreign taxes" means value-added taxes and custom duties assessed by a foreign government on a commodity. It does not include foreign sales taxes.
(d) Where. Submit the reports to: tax-indo@usaid.gov with a copy to the Contracting Officer Representative (COR).
(e) Sub-agreements. The Contractor must include this reporting requirement in all applicable subcontracts, sub-grants and other sub-agreements.
(f) For further information see http://2001-2009.state.gov/s/d/rm/c10443.htm.

AIDAR 752.231-71 SALARY SUPPLEMENTS FOR HOST GOVERNMENT (HG) EMPLOYEES (MAR 2015)

(a) Salary supplements are payments made that augment an employee's base salary or premiums, overtime, extra payments, incentive payment and allowances for which the HG employee would qualify under HG rules or practice for the performance of his/hers regular duties or work performed during his/hers regular office hours. Per diem, invitational travel, honoraria and payment for work carried out outside of normal working hours are not considered to be salary supplements.

(b) Salary supplements to HG Employees are not allowable without the written approval of the contracting officer.

(c) The Contractor must insert a clause containing all the terms of this clause, including the requirement to obtain the written approval of the contracting officer for all salary supplements, in all subcontracts under this contract that may entail HG employee salary supplements.

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) http://www.arnet.gov/far and (AIDAR) http://www.usaid.gov/ads/policy/300/aidar

NUMBER	TITLE	DATE
	FEDERAL ACQUISITION REGULATION	
52.202-1	DEFINITIONS	NOV 2013
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	MAY 2014
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	SEP 2006
52.203-7	ANTI-KICKBACK PROCEDURES.	MAY 2014

52.203-8	CANCELLATION, RESCISION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY	MAY 2014
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	OCT 2010
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	OCT 2015
52.203-15	WHISTLEBLOWER PROTECTIONS UNDER THE AMERICAN RECOVERY AND REINVERSTMENT ACT OF 2009	JUN 2010
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER	APR 2014

52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES	JUL 2018
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	OCT 2015
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS	NOV 2015
52.215-10	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA	AUG 2011
52.215-11	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA – MODIFICATIONS	AUG 2011
52.215-12	SUB-CONTRACTOR CERTIFIED COST OR PRICING DATA (DEVIATION 2018-O0015)	MAY 2018
52.215-13	SUB-CONTRACTOR CERTIFIED COST OR PRICING DATA – MODIFICATIONS (DEVIATION 2018-O0015)	MAY 2018
52.215-19	NOTIFICATION OF OWNERSHIP CHANGES	OCT 1997
52.222-3	CONVICT LABOR	JUN 2003
52.222-21	PROHIBITION OF SEGREGATED FACILITIES	APR 2015
52.222-26	EQUAL OPPORTUNITY	SEPT 2016
52.223-6	DRUG-FREE WORKPLACE	MAY 2001
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	JUN 2008
52.225-25	PROHIBITION ON CONTRACTING WITH ENTITIES ENGAGING IN CERTAIN ACTIVITIES OR TRANSACTIONS RELATING TO IRAN-REPRESENTATION AND CERTIFICATION	OCT 2015
52.227-14	RIGHTS IN DATA – GENERAL	MAY 2014
52.227-23	RIGHTS TO PROPOSAL DATA (TECHNICAL)	JUN 1987
52.228-7	INSURANCE - LIABILITY TO THIRD PERSONS	MAR 1996
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
52.233-1	DISPUTES Alternate I (Dec 1991)	MAY 2014
52.242-13	BANKRUPTCY	JUL 1995
52.243-7	NOTIFICATION OF CHANGES	JAN2017
52.246-25	LIMITATION OF LIABILITY – SERVICES	FEB 1997
52.247-63	PREFERENCE FOR U.S. FLAG AIR CARRIERS	JUN 2003

AIDAR 48 CFR CHAPTER 7

752.209-71	ORGANIZATIONAL CONFLICTS OF INTEREST DISCOVERED AFTER AWARD	JUN 1993
752.211-70	LANGUAGE AND MEASUREMENT	JUN 1992
752.227-14	RIGHTS IN DATA – GENERAL	OCT 2007
752.228-7	INSURANCE – LIABILITY TO THIRD PERSONS	JUL 1997
752.245-70	GOVERNMENT PROPERTY - USAID REPORTING REQUIREMENTS	OCT 2017
752.7037	CHILD SAFEGUARDING STANDARDS	AUG 2016
752.7038	NONDISCRIMINATION AGAINST END-USERS OF SUPPLIES OR SERVICES	OCT 2016

I.2 FAR 52.222-36 EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUL 2014)

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

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

[Class Deviation- 2017-O0008, Office of Federal contract Compliance Programs Waiver of Certain Clause Requirements in Contracts for Hurricane Harvey Relief Efforts. This clause deviation is effective on Sept 01, 2017, and remains in effect until incorporated into the FAR, or otherwise rescinded.

(f)Notwithstanding the provisions of this section, the Contractor will not be obligated to develop the written affirmative action program required under the regulations implementing section 503 of the Rehabilitation Act of 1973, as amended.

I.3 AIDAR 752.222-70 USAID DISABILITY POLICY – ACQUISITION (DECEMBER 2004)

(a) The objectives of USAID Disability Policy are (1) to enhance the attainment of United States foreign assistance program goals by promoting the participation and equalization of opportunities of individuals with disabilities in USAID policy, country and sector strategies, activity designs and implementation; (2) to increase awareness of

issues of people with disabilities both within USAID programs and in host countries; (3) to engage other U.S. government agencies, host country counterparts, governments, implementing organizations and other donors in fostering a climate of nondiscrimination against people with disabilities; and (4) to support international advocacy for people with disabilities. The full text of the policy paper can be found at the following website: http://pdf.usaid.gov/pdf_docs/PDABQ631.pdf.

(b) USAID therefore requires that the Contractor not discriminate against people with disabilities in the implementation of USAID programs and that it make every effort to comply with the objectives of USAID Disability Policy in performing this contract. To that end and within the scope of the contract, the Contractor's actions must demonstrate a comprehensive and consistent approach for including men, women and children with disabilities.

I.4 AIDAR 752.229-71 REPORTING OF FOREIGN TAXES (JULY 2007)

(c) The Contractor must annually submit a report by April 16 of the next year.
(d) Contents of Report. The reports must contain:

a. Contractor name.
b. Contact name with phone, fax number and e-mail address.
c. Contract number(s).
d. Amount of foreign taxes assessed by a foreign government [each foreign government must be listed separately] on commodity purchase transactions valued at
$500 or more financed with U.S. foreign assistance funds under this agreement during the prior U.S. fiscal year.
e. Only foreign taxes assessed by the foreign government in the country receiving
U.S. assistance are to be reported. Foreign taxes by a third party foreign government are not to be reported. For example, if a contractor performing in Lesotho using foreign assistance funds should purchase commodities in South Africa, any taxes imposed by South Africa would not be reported in the report for Lesotho (or South Africa).
f. Any reimbursements received by the Contractor during the period in paragraph
(g) (4) of this clause regardless of when the foreign tax was assessed and any

reimbursements on the taxes reported in paragraph (b)(4) of this clause received through March 31.
g. Report is required even if the Contractor did not pay any taxes during the reporting period.
h. Cumulative reports may be provided if the Contractor is implementing more than one program in a foreign country.

(h) Definitions. As used in this clause --

(1) "Agreement" includes USAID direct and country contracts, grants, cooperative agreements and interagency agreements.
(2) "Commodity" means any material, article, supply, goods, or equipment.
(3) "Foreign government" includes any foreign governmental entity.
(4) "Foreign taxes" means value-added taxes and custom duties assessed by

a foreign government on a commodity. It does not include foreign sales taxes.

(i) Where. Submit the reports to: tax-indo@usaid.gov with a copy to the Contracting Officer Representative (COR).

(j) Sub-agreements. The Contractor must include this reporting requirement in all applicable subcontracts, sub-grants and other sub-agreements.

(k) For further information see http://2001-2009.state.gov/s/d/rm/c10443.htm.

ANNEX F – Quick Start Guide for Getting a Unique Entity ID (SAM)

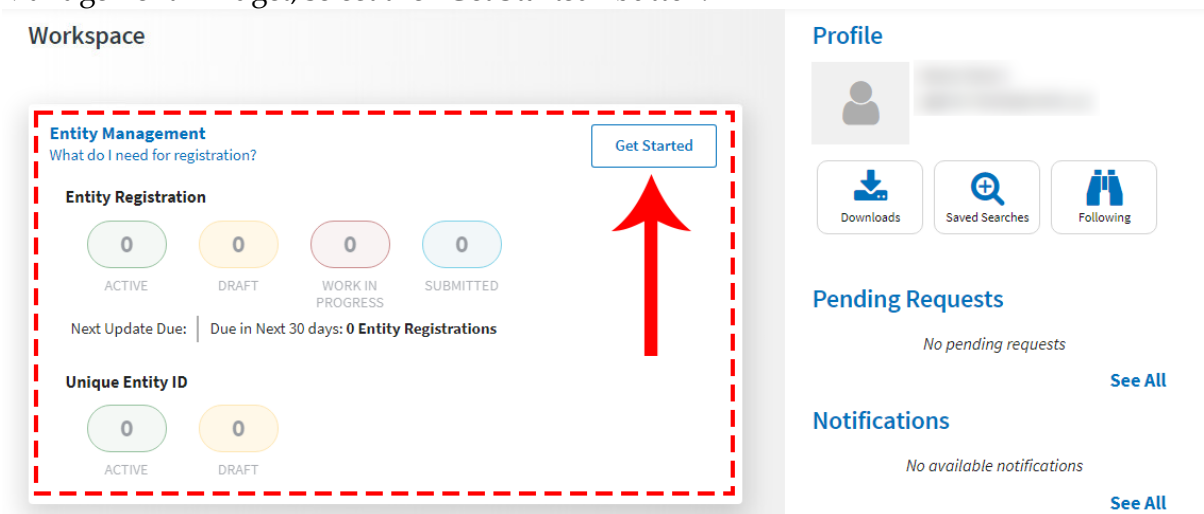
You can get a Unique Entity ID (SAM) for your organization without having to complete a full entity registration. If you only conduct certain types of transactions, such as reporting as a sub-awardee, you may not need to complete an entity registration. Your entity may only need a Unique Entity ID (SAM).

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

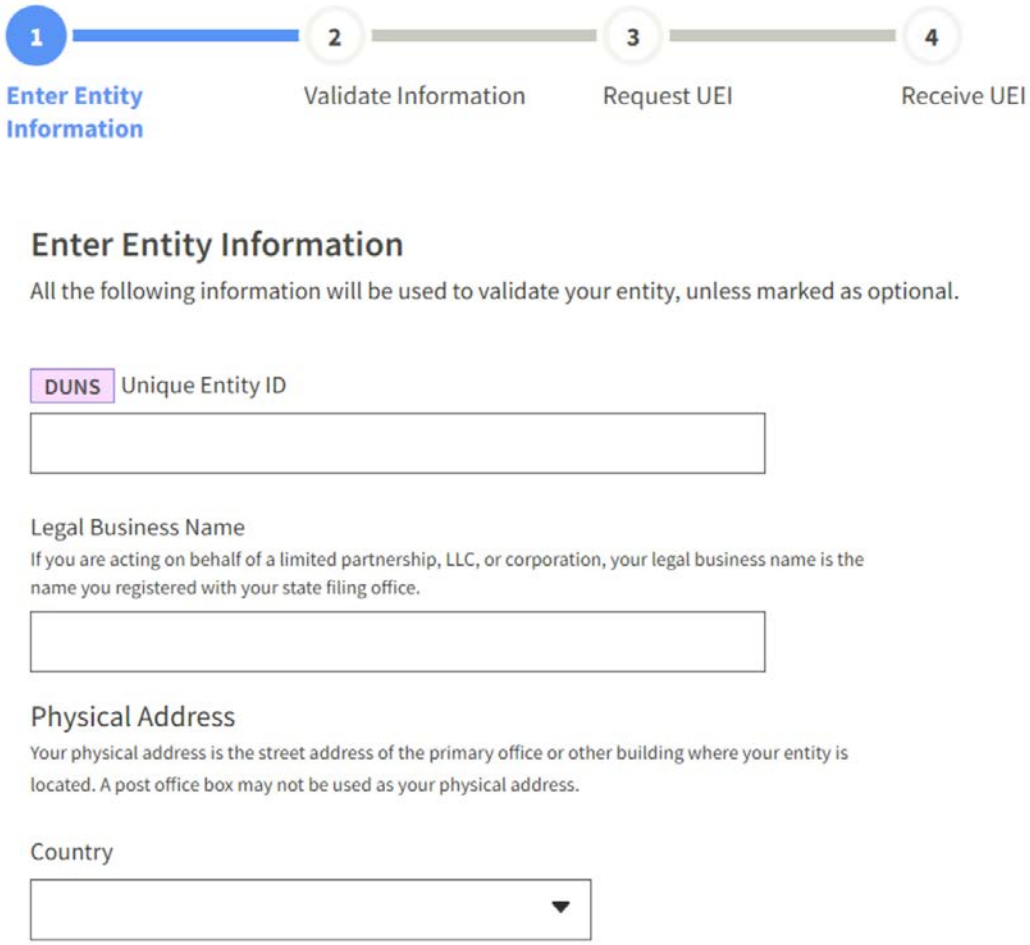
Your entity has a DUNS Number and is registered in SAM.gov
If you have an active or inactive registration in SAM.gov today, you've already been assigned a Unique Entity ID (SAM). It's viewable on your entity registration record in SAM.gov. Learn how to view your Unique Entity ID (SAM) here.

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

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. More help with using Login.gov can be accessed here. 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.

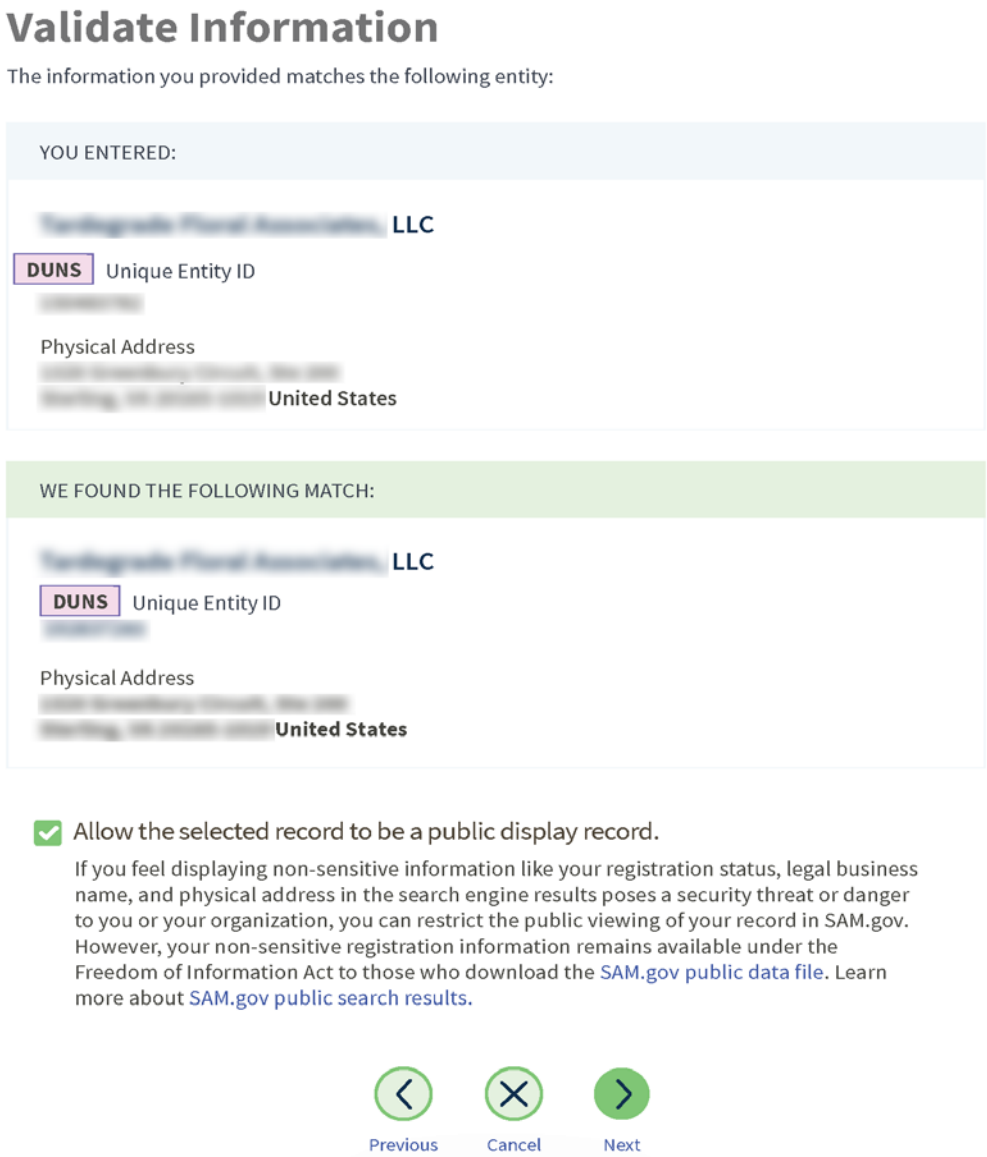


3. On the next page, enter information about your entity. All fields are required, unless marked as optional.

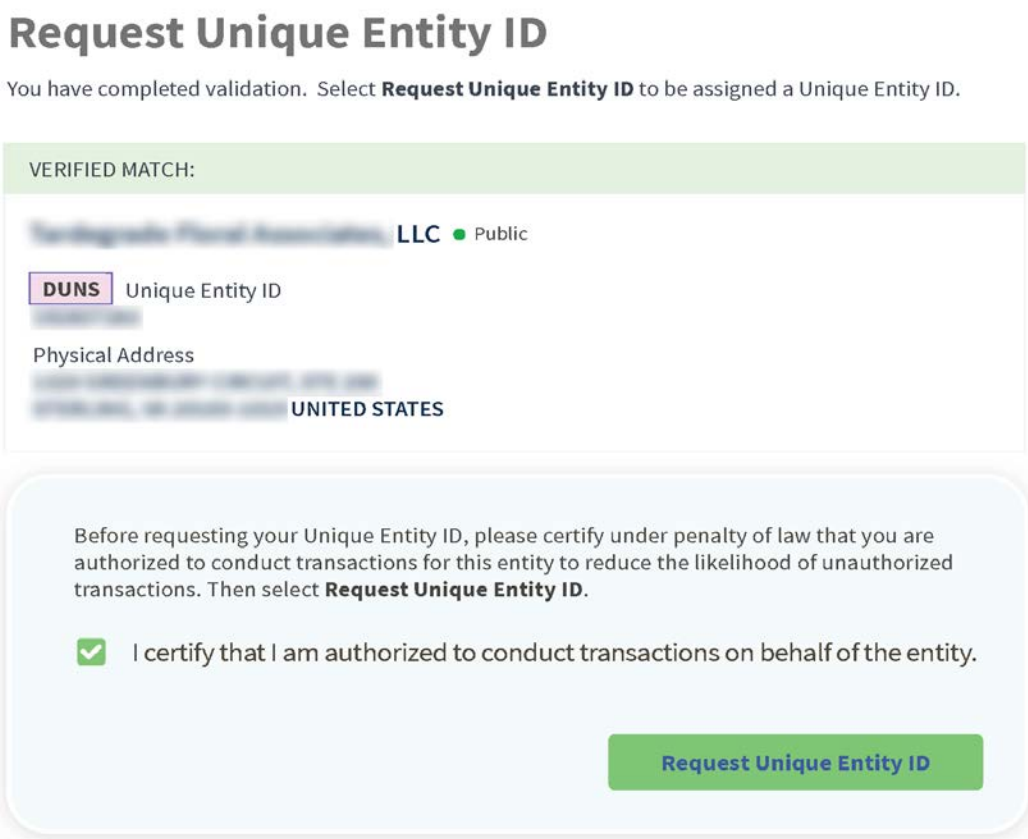


4. On the next page, validate that the information provided is correct. If the information provided does not match your Dun & Bradstreet record exactly, you will be able to proceed. For assistance updating your Dun & Bradstreet record, please contact Dun & Bradstreet.

   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 (SAM) record. Other entities and users of SAM.gov will not be able to view your Unique Entity ID (SAM) record. 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 (SAM) will be displayed and you can begin to use it for your entity.

Your entity does not have a DUNS Number and today's date is <u>before</u> April 4, 2022

Before April 4, 2022, the DUNS Number issued by Dun & Bradstreet is the authoritative entity identifier used by the federal government. You need to get a DUNS Number first before you can request a Unique Entity ID (SAM).

Go to fedgov.dnb.com/webform to request a free DUNS Number. It can take 1-2 business days before your DUNS Number is issued. When you are assigned your DUNS Number, return to SAM.gov and follow the steps outlined under the "**Your entity has a DUNS Number and is not registered in SAM.gov**" section of this guide.

Your entity does not have a DUNS Number and today's date is after April 4, 2022

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