DEVTECH
Innovative Solutions for Development

REQUEST FOR PROPOSAL

RFP No. CATALYZE-EXTERNAL-MEL-2023 – 001

CONTRACT:	CATALYZE External MEL IDIQ
TYPE OF SUBCONTRACT	Fixed Price Subcontract
PROJECT/Task Order:	CATALYZE TO 3 – Tool Validation
ESTIMATED BUDGET CEILING:	20,000 USD each Country. DevTech expects to issue up to 4 awards
SUPERVISOR(s)	Carla Paredes
PLACE OF PERFORMANCE:	Rwanda, Tanzania, South Africa, and Zambia
QUESTION AND ANSWER PERIOD:	February 5th – February 10th, 2022
FINAL SUBMISSION OF PROPOSAL DUE BY:	February 17, 2023, 5:00 p.m. EST
TENTATIVE START DATE:	March 6, 2023
COMPLETION DATE:	April 21, 2023

DevTech Systems, Inc. (DevTech) is an international consulting firm dedicated to development, with over 38 years of experience providing advisory services and technical assistance to government, private sector, and civil society stakeholders in more than 100 countries. We are a data driven organization that specializes in informing policy making by delivering focused data-driven evidence-based analysis products and services. DevTech core practice areas include Economic and Data analysis, Monitoring and Evaluation, Education and Youth Development, Gender and Inclusive Development, and Public Financial Management.

DevTech is a sub-contractor to Palladium, under the CATALYZE EduFinance External Monitoring Evaluation and Learning (MEL) IDIQ. DevTech is currently designing independent impact evaluations to measure the association between CATALYZE EduFinance activities in Sub-Saharan Africa countries and change in education outcomes. Findings of the evaluations aim to strengthen implementation and support adaptive management and learning of EduFinance activities and inform future activity design.

Under the external MEL IDIQ, **DevTech is soliciting proposals to hire four research institutions to translate, test, and validate data collection tools approved to measure education outcomes in four countries: Rwanda, South Africa, Tanzania, and Zambia.** The tools will be used in future impact evaluations of the CATALYZE EduFinance activities. Please submit your most competitive proposals in accordance with the instructions for offers and terms of reference. Any award issued as a result of this RFP will be subject to all instructions, terms of reference/specifications, certifications, terms and conditions, and funder-required clauses.

I. BACKGROUND

The CATALYZE Blended Finance Mechanism is a $250 Million, 8-year contract (5-year base period, with a single 3-year option period) which uses a facilitated partnership model to craft solutions to crowd in $2 Billion in blended finance (i.e. blended concessional and commercial finance) to USAID partner countries and initiatives. CATALYZE allows USAID Bureaus and Missions to efficiently deploy investment facilitation solutions that respond to the needs of specific sectors, issues, and geographies. Initial programs focus on education finance to implement sustainable education business models serving low-income communities, and achievement of the W-GDP objectives, but the mechanism can be applied to any development challenge or region.

The first USAID Bureau to buy-in to CATALYZE was the Bureau for Economic Growth, Education and Environment (E3) which led to the creation of the CATALYZE EduFinance mechanism. The aim of this mechanism is to improve the educational and learning outcomes in disadvantaged children and youth by mobilizing private capital for the non-state education sector. Under this mechanism, USAID is funding public-private sector partnerships (PPPs) and private sector activities in several countries (hereafter called "EduFinance activities"). Independent evaluations will be conducted of these EduFinance activities in order to determine if the goals and intermediate results have been met. The main interventions and target beneficiaries vary depending on the country and the Implementing Partner. Overall, there are three types: (i) school improvement loans to schools; (ii) school fee loans to parents; and (iii) education quality improvement through the professional development of school managers and teachers as well as school development planning. Interventions focus on pre-primary education and primary education.

Local ownership of the evaluation process and use of results will be an important objective of each evaluation. All evaluations will accordingly be designed and conducted in consultation and collaboration with local stakeholders and will focus on a set of overarching and locally relevant evaluation questions.

Findings of the evaluations will be used to strengthen implementation and support adaptive management and learning of EduFinance activities and inform future activity design. In addition, the synthesis of the evaluations will be shared with key stakeholders, such as Congress and the EduFinance Community of Practice, in order to expand the body of evidence about Private Sector Engagement (PSE) initiatives strengthening development outcomes.

As part of a landscape analysis conducted in year 2022, DevTech identified the methodologies used to assess learning outcomes of primary and pre-primary learners attending non-state educational facilities in the EduFinance countries and assessed the feasibility of using the Annual Status of Education Report (ASER), Early Learning Outcome Measure (ELOM), Measuring Early Learning and Quality Outcomes (MELQO), among other tools. Results of the analysis resulted in the selection of MELQO for Rwanda and Tanzania, ELOM for South Africa and ASER for Zambia.

2. SCOPE OF WORK

2.1. Objective

The research institution will translate, test, and validate data collection tools approved to measure education outcomes in one of the following countries: Rwanda, South Africa, Tanzania and Zambia.

The tools will be used for education assessments at specific provinces within each country where EduFinance Activities are implemented. Translation from English is required in the following languages:

- Zambia: Cinyanja, plus one other local language still to be determined (can be Icibemba or Chitonga).
- Tanzania: Kiswahili
- Rwanda: Kinyarwanda
- South Africa: TBD

2.2. Inputs

DevTech will provide the following inputs, all in English:

- ASER tool with application instructions
- MELQO (both MODEL and MELE tools) with application instructions
- Complementary questionnaires (to collect information on relevant covariates). Complementary questionnaires include:
  - Teacher questionnaire to get information about teacher characteristics and experience
  - Learner questionnaire to get information about learner-associated factors that might influence learning outcomes (mother tongue, age, support from their families, etc.)
  - School inventory questionnaire to get information about school characteristics, including infrastructure topics.

All inputs will be provided in Microsoft Word and/or Microsoft Excel editable files.

2.3. Tasks

Task 1. Take stock of all inputs and what is available already in local languages where CATALYZE intervention is taking or will take place.

Task 2. Develop a workplan for the tool validation. This will include description of activities, timelines, costs and personnel required to complete the task.

Task 3. Draft a localized version of the complementary questionnaires for learners, teachers and school characteristics that DevTech provides. For South Africa, collect the ELOM learning assessment tools in English. Submit instruments to DevTech for review and approval:

a) Draft ELOM Tools in English for South Africa.
b) Complementary questionnaires to be used as part of the data collection for baseline and endline evaluations in each country.

Task 4. Develop a **testing plan** for each tool. The plan must include translation of tools in required local language(s), the timeline, and methodology for testing describing who will be administering the tool and who will be using it (who will be assessed during the tool testing).

The local institution will then incorporate client feedback on tools to finalize them and receive DevTech's approval to proceed.

Task 5. Translate and adapt the approved tools to local languages and culture, as needed, and validate translated tools with local stakeholders. Local stakeholders may include (but are not limited to) MOE staff, teachers, Implementing Partners, and non-government organizations working on education. Participants should have experience in early childhood education and primary level education and should be fluent in the local languages that the tools were translated to. Languages will include, at minimum, the following:

- Zambia: Cinyanja, plus one other local language still to be determined (TBD).
- Tanzania: Kiswahili
- Rwanda: Kinyarwanda
- South Africa: TBD

Task 6. Test the **translated data collection instruments** in accordance with the approved testing plan, and update DevTech and the client on relevant findings of the test in the form of a brief report. This may require updating and modifying survey instruments in accordance with findings from the pre-tests to make them implementation ready.

3. ORGANIZATIONAL MINIMUM REQUIREMENTS

The organization should possess the following experience and qualifications

1) Institutional and financial capacity to perform all duties outlined in this scope of work.
2) Certified, legally registered entity, and by law has the capacity to sign a contract
3) Not under court supervision due to bankruptcy or business activity being discontinued
4) Not affiliated with any criminal associations or activity
5) Verified references that document work performed on at least five similar jobs
6) Knowledge of the target country education system

7) Experience conducting research in education in the target country
8) Experience administering the data collection tools a plus
9) Familiarity with the data collection tools a plus
10) UEI number as required to work with the US Government

4. KEY PERSONNEL

The Offeror should provide at minimum the following key personnel with the following qualifications

1) **Local Research/Contract Coordinator.** Main point of contact between DevTech and the local organization. Responsible for providing technical leadership to the local team, and any other technical requirements. Minimum qualifications include:
   - A minimum of a master's degree in areas related to development, education, research or evaluation
   - Five years' experience working on the education sector, preferably conducting assessments at the primary and/or pre-primary level.
   - Deep understanding of the education sector in your country and knowledge of local education stakeholders
   - Demonstrable research skills such as data analytics, statistics, or survey design.
   - Impeccable writing and organizational skills
   - Fluency in written and spoken English and local language

2) **2 Lingüistic Experts.** Will support the translation, validation, and contextualization of tools.
   - Native speaker of the local language that the tools will be translated into
   - Experience working in the education sector
   - Knowledge of education assessments, preferably using tools such as MELQO, ASER or ELOM

The offeror can provide more personnel within their staffing plan, as needed, to ensure that the tasks are finalized in time.

5. DELIVERABLES

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

Work plan (Deliverable 1) must be delivered to DevTech, Inc. within two weeks of contract signing. The work plan must be a comprehensive document (10-15 pages) including:

- Proposed detailed activities for the entire period of performance, including a timeline of activities.
- Proposed due dates of submission of deliverables as outlined in this Section.
- Proposed cost and personnel to carry out all of the activities under the subcontract.

For South Africa only. ELOM data collection tools in English (Deliverable 2). Tools should be delivered in editable, Microsoft Word Documents for review. The tools should include the following:

- Draft ELOM Tools in English for South Africa
  - ELOM Assessment Tool 4 & 5 Years
  - ELOM Assessment Tool 6 & 7 Years

- ELOM Learning Program Quality Tool
- ELOM Assessment Manuals
- ELOM Scoring sheet
- Complementary questionnaires for learners, teachers and school characteristics

Testing Plan (Deliverable 3). The plan must include a step-by-step process and timeline methodology to test ELOM, MELQO and ASER translated tools in respective countries. The plan should include a clear pathway to translate the tools, obtain local stakeholders and client feedback, and make them ready to implement locally.

Final data collection tools in English and Local Languages (Deliverable 4). Final tools should be delivered in editable, Microsoft Word Documents.

6. PAYMENT SCHEDULE

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

Deliverable	Payment	Due Date
Deliverable 1. Work Plan	15%	2 weeks after signing the contract
Deliverable 2 and 3. ELOM data collection tools for South Africa in English and Testing plan for all countries	35%	5 weeks after signing the contract
Final data collection tools in English and Local Languages, including ASER, MELQO, ELOM and Complementary Questionnaires	50%	8 weeks after signing the contract
Total	**100%**	

All deliverables must be approved by DevTech's Supervisor prior to payment.

7. PROPOSAL SUBMISSION REQUIREMENTS

The offeror's proposal must be accompanied by a cover letter typed on official organizational letterhead and signed by an individual who has signatory authority for the offeror. The offeror must submit a complete proposal package on or before the due date and time indicated on page 1 to the emails in Section 8. Submission Instructions. Proposals must be submitted by email only and with the subject line CATALYZE-EXTERNAL-MEL-2023 – 001

The proposals must be prepared in two separate volumes: i) Technical Proposal; and ii) Cost Proposal. The technical and cost proposal must be kept separate. Technical proposals must not make reference or include any pricing data to evaluate the technical proposal strictly on the basis of technical merit.

The written proposal must contain the following information and documentation:

7.1. Technical Proposal

The Technical proposal shall describe how the offeror intends to accomplish all of the requirements stated in the Scope of Work. It should be concise, specific, complete, and demonstrate a clear understanding of the work to be undertaken and the responsibilities of all parties involved. It must demonstrate the offeror's eligibility, as well as their capabilities and expertise in conducting each step of the activity.

Offerors shall include only information necessary to provide a clear understanding of the proposed action and the justification for it. Greater detail than necessary, as well as insufficient detail may detract from a proposal's clarity. Assume that the reader is not familiar with the context in which the project will be implemented. Minimize or avoid the use of jargon and acronyms as much as possible. If acronyms or abbreviations are used, include a separate page explaining the terms.

The Technical Proposal should include the following sections:

1. **Organization Overview** - Legal name; year of incorporation; number of employees; description of all services and products supplied.
2. **Narrative** outlining how the applicant will successfully complete activities and responsibilities outlined in the scope of work. (up to five pages)
3. **Capabilities and Past Performance** - Description of applicable organizational capabilities/experience and major accomplishments in conducting job similar in size and complexity outlined in this scope of work in the last 5 years. Information of similar jobs should include funding agency and cost (up to three pages)
4. **Staffing Plan** - Provide a proposed staffing plan to develop policy briefs, policy papers, and manage the workshops and conference outlined in this SOW.
5. **Curriculum Vitae** of proposed key personnel (up to two pages each) along with three references each.
6. **Contact information** of three recent clients for similar activities. Please provide name, email and phone contact information.

Proposal should be no longer than 10 pages, excluding CVs.

7.2. Cost Proposal

The offeror should submit their most competitive and complete cost proposal. The cost proposal shall be submitted in a separate volume from the technical proposal. The cost proposal shall be submitted as a firm-fixed price proposal in United States currency. The cost proposal shall include the following:

A. Cover sheet with organization information, including name, address, email, phone, Unique Entity ID number, and contact person. If your organizations does not have a UEI , you will need to request one which you can do for FREE at www.sam.gov. For more information, please visit, https://sam.gov/content/duns-uei or https://www.fsd.gov/gsafsd_sp?id=kb_article_view&sysparm_article=KB0038428&sys_kb_id=3fcba40b1b0a01d40ca4a97ae54bcbd7&spa=1
B. Audited Financial Statements for the past three years.
C. Evidence of Responsibility (see Annex A)
D. Certification Regarding Debarment, Suspension, or Proposed Debarment (see Annex C)
E. Representations, Certifications, and Other Statements of Bidders & Other Contract Clauses (see Annex B)
F. A budget in Excel with the Offeror's fixed price for each deliverable, each of which will be considered a fixed price budget for that specific segment of work. The price to be awarded will be an all-inclusive fixed price. No profit, fee or additional costs can be included after the award.

All items/services must be clearly labeled and included in the total offered price. The budget must be completed in the attached budget template (see Annex E). It should include three tabs 1) Fixed price 2) Summary 3) Detailed budget. Any assumptions can be included in tab 4. Detailed budget shall include, at minimum: wages, travel and transportation, and other direct costs. Proposed budget will be structured in accordance to the payment schedule in Section 6 above. Applicants are to include all costs deemed necessary to execute this SOW in the application budget.

G. A detailed budget narrative in word or pdf that justifies the cost as appropriate and necessary for the successful completion of proposed activities and deliverables. The budget narrative should clearly describe the project and cost assumptions. All proposed costs must be directly applicable to performing the work under the award and budgeted amounts should not exceed the market cost/value of an item or service. The budget narrative should be of sufficient detail so that someone unfamiliar with your organization or the activity could review and adequately understand and grasp the assumptions, reasonableness and calculation method used.

H. Information Concerning Work-Day, Work-Week, and Paid Absences: The Offeror shall indicate the number of hours and days in its normal workday and its normal workweek, both domestically and overseas, for employees and consultants. In addition, the Offeror shall indicate how paid absences (US holidays, local holidays, vacation and sick) shall be covered. A normal work-year, including paid absences (holidays, vacations, and sick leave) is 2,080 hours (260 days x 8 hours per day). However, some organizations do not have an 8-hour workday, and some accounting systems normally provide for direct recovery of paid absences by using a work-year of less than 2,080 hours to compute individuals' unburdened daily rates. The Offeror shall describe their workday and workweek policies. The workday and work-week policies and the method of accounting for paid absences for the Offeror in effect at the time of award shall remain enforce throughout the period of the award. The Offeror may use template in Annex D or provide their own template with the same information.

7.3. Submission Instructions

All questions and final proposal should be submitted by the dates established on page 1 to mnunez@devtechsys.com. No late submissions will be accepted.

7.4. Language

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

7.5. Proposal Evaluation Criteria

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

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

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

Evaluation factors are as follows:

No.	Criteria	Points
1	Demonstrated understanding of the Scope of Work	30
2	Capabilities and Past Performance: Previous experience and demonstrated capabilities coordinating and managing research and events in similar size and complexity	15
3	Relevant experience of proposed personnel to deliver SOW tasks	30
4	Proposed costs	25
	Total	**100**

8. TERMS OF AWARD

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

All deliverables produced under the future award/sub-contract shall be considered the property of DevTech. DevTech may choose to award a sub-contract for part of the activities in the RFP.

9. PROPOSAL VALIDITY

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

10. PAYMENT TERMS

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

11. FINANCIAL RESPONSIBILITY

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

12. AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this award is "935". Local procurements are to be accomplished in accordance with AIDAR 752.225-71 and ADS 311. Geographic Code 935 is defined as any area or country including the cooperating country, but excluding foreign policy-restricted countries.

13. NEGOTIATIONS

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

14. REJECTION OF PROPOSALS

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

15. INCURRING COSTS

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

16. MODIFICATIONS

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

17. CANCELLATION

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

18. USAID REGULATIONS

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

DEVTECH
Innovative Solutions for Development

ANNEX A

Evidence of Subcontractor/Subrecipient Responsibility Statement

1. Authorized Negotiators

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

(List Names of Authorized signatories)

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

Address
Tel
Email

2. Adequate Financial Resources

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

3. Ability to Comply

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

4. Record of Performance, Integrity, and Business Ethics

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

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

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

6. Equipment and Facilities

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

DEVTECH
Innovative Solutions for Development

7. Eligibility to Receive Award

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

8. Cognizant Government Audit Agency

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

9. Recovery of Vacation, Holiday and Sick Pay

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

Date:_____

Name:_____

Title: _____

Authorized Signature:_____

Unique Entity ID:_____

DEVTECH
Innovative Solutions for Development

ANNEX B

Representations, Certifications, and Other Statements of Bidders & Other Contract Clauses

5. TERMS OF THE PRIME CONTRACT AND TASK ORDER

5.1. Contract Clauses Specifically Incorporated by Reference. The Subcontract incorporates, to the fullest extent possible, the following Federal Acquisition Regulation ("FAR") and USAID Acquisition Regulation ("AIDAR") requirements. Where the FAR or AIDAR clause uses the term "government" or "contracting officer", the words "and DevTech" shall be added. Where the FAR or AIDAR clauses uses the term "contractor," the word "subcontractor" shall be substituted unless otherwise noted below.

5.1.2. Restrictions on Subcontractor Sales to The Government. The Prime Contract includes FAR 52.203-6 (Restrictions on Subcontractor Sales to The Government (SEP 2006)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.203-6 as if the clause were set forth in full text in this Subcontract.

5.1.3. Contractor Code of Business Ethics and Conduct. The Prime Contract includes FAR 52.203–13 (Contractor Code of Business Ethics and Conduct (June 2020) (Pub. L. 110–252, Title VI, Chapter 1 (41 U.S.C. 251 note))), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.203–13 as if the clause were set forth in full text in this Subcontract.

5.1.4. Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights. The Prime Contract includes FAR 52.203-17 (Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights DEVIATION M-OAA-DEV-FAR-18-Ic (June 2020)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.203-17 as if the clause were set forth in full text in this Subcontract.

5.1.5. Reporting Executive Compensation and First-Tier Subcontract Awards. The Prime Contract includes FAR 52.204-10 (Reporting Executive Compensation and First-Tier Subcontract Awards (June 2020)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of 52.204-10 as if the clause were set forth in full text in this Subcontract, except that Subcontractor will provide all required information to **DevTech** at least two weeks prior to deadlines set forth therein.

5.1.6. Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. The Prime Contract includes FAR 52.209-6 (Protective Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.209-6 as if the clause were set forth in full text in this Subcontract.

5.1.7. Prohibition on Contracting with Entities That Require Certain Internal Confidentiality Agreements. The Prime Contract includes FAR 52.203-99 (Prohibition on Contracting with Entities That Require Certain Internal Confidentiality Agreements (Deviation 2015-02) (April 2015)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.203-99 as if the clause were set forth in full text in this Subcontract.

5.1.8. Combating Trafficking in Persons. The Prime Contract includes FAR 52.222-50 (Combating Trafficking in Persons), which is hereby incorporated by reference in this Subcontract. The

Subcontractor shall comply with all applicable provisions of FAR 52.222-50 as if the clause were set forth in full text in this Subcontract.

5.1.9. Nondiscrimination Against End-Users of Supplies or Services. The Prime Contract includes AIDAR 752.7038 (Nondiscrimination Against End-Users of Supplies or Services October 2016), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of AIDAR 752.7038 as if the clause were set forth in full text in this Subcontract.

5.1.10. Worker's Compensation Insurance. The Prime Contract includes AIDAR 752.228-3 (Worker's Compensation Insurance (Defense Base Act). (Dec 1991)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of AIDAR 752.228-3 as if the clause were set forth in full text in this Subcontract.

5.1.14. Information Technology Approval. All IT procurements proposed to be included in the price of the Task Orders must be clearly identified in the proposal for every Task Order.

5.1.15. Media and Information Handling and Protection. The Prime Contract (Media and Information Handling and Protection (APRIL 2018)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of Clause H.23 as if the clause were set forth in full text in this Subcontract.

5.1.16. Privacy and Security Information Technology Systems Incident Reporting. The Prime Contract includes Clause H.24 (Privacy and Security Information Technology Systems Incident Reporting (APRIL 2018)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of Clause H.24 as if the clause were set forth in full text in this Subcontract.

5.1.17. Security Requirements for Unclassified Information Technology Resources. The Prime Contract includes Clause H.26 (Security Requirements for Unclassified Information Technology Resources (APRIL 2018)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of Clause H.26 as if the clause were set forth in full text in this Subcontract.

5.1.18. Cloud Computing. The Prime Contract includes Clause H.27 (Cloud Computing (APRIL 2018)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of Clause H.27 as if the clause were set forth in full text in this Subcontract.

5.1.19. Cloud Computing. The Prime Contract includes FAR 52.204-23 (Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (April 2018)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of FAR 52.204-23 as if the clause were set forth in full text in this Subcontract.

5.1.20. Source and Nationality Requirements. The Prime Contract includes AIDAR 752.225-70 (Source and Nationality Requirements (FEB 2012)), which is hereby incorporated by reference in this Subcontract. The Subcontractor shall comply with all applicable provisions of AIDAR 752.225-70 as if the clause were set forth in full text in this Subcontract.

5.2. Other Clauses Incorporated by Reference. This Subcontract incorporates terms of the Prime Contract. Prime Contractor and Subcontractor shall comply with all such clauses with the same force and effect as if they were given in full text herein.

5.3. Order of Precedence. The clauses incorporated in this Subcontract shall, to the greatest extent possible, be deemed to be cumulative to the terms, conditions, and requirements of this Subcontract. In the case of an irreconcilable conflict between this Subcontract and Task Order including FAR and AIDAR

clauses, the provisions of this Subcontract shall control. Federal Law and Clauses take precedent over state laws except where state laws are specifically invoked in this Subcontract.

6.2. Lower-Tier Subcontracting. Subcontractor shall not enter into any lower- tier Subcontract for any portion of this Subcontract without first obtaining **DevTech's** written approval thereof; provided, however, that this limitation shall not apply to Subcontractor's purchase of standard commercial supplies. Any lower-tier subcontract awarded shall be consistent with the objective of this Subcontract, the Prime Contract, the Task Order, the FAR, and the AIDAR.

INCORPORATED REGULATORY PROVISIONS

The Federal Acquisition Regulation (FAR) clauses referenced below are incorporated herein by reference, with the same force and effect as if they were given in full text, and are applicable, including any notes following the clause citation, to this Subcontract. If the date or substance of any of the clauses listed below is different from the date or substance of the clause actually incorporated in the Prime Subcontract referenced by number herein, the date or substance of the clause incorporated by said Prime Subcontract shall apply instead. The Contracts Disputes Act shall have no application to this Subcontract, and nothing in this Subcontract grants Subcontractor a direct claim or cause of action against the U.S. Government. Any reference to a "Disputes" clause shall mean the "Disputes" clause of this Subcontract. Subcontractor shall include in each lower-tier the appropriate flow down clauses as required by the FAR and FAR Supplement clauses included in this Subcontract.

1.1 GOVERNMENT

(a) This Subcontract is entered into by the parties in support of a U.S. Government contract.
(b) As used in the FAR clauses referenced below and otherwise in this Subcontract:
1) "Commercial Item" means a commercial item as defined in FAR 2.101.
2) "Commercially available off-the-shelf (COTS) item" means a COTS item as defined in FAR 2.101.
3) "Agreement" means this Subcontract.
4) "Contracting Officer" shall mean the U.S. Government Contracting Officer for Company's government prime contract under which this Subcontract is entered.
5) "Subcontractor" and "Offeror" means Subcontractor, which is the party identified on the face of the Subcontract with whom DevTech is contracting, acting as the first-tier subcontractor to the Prime.
6) "Prime Subcontract" means the contract between Company and the U.S. Government or between Company and its higher-tier contractor who has a contract with the U.S. Government.
7) "Subcontract" means any contract placed by the Subcontractor or lower-tier subcontractors under this Subcontract.

1.2 NOTES

(a) The following notes apply to the clauses incorporated by reference below only when specified in the parenthetical phrase following the clause title and date.
1) Substitute "Company" for "Government" or "United States" throughout this clause.
2) Substitute "Company Contracting Representative" for "Contracting Officer", "Administrative Contracting Officer", and "ACO" throughout this clause.
3) Insert "and Company" after "Government" throughout this clause.
4) Insert "or Company" after "Government" throughout this clause.
5) Communication/notification required under this clause from/to Subcontractor to/from the Contracting Officer shall be through Company.
6) Insert "and Company" after "Contracting Officer", throughout the clause.
7) Insert "or Company Contracting Representative" after "Contracting Officer", throughout the clause.

(b) See also the clause of this Subcontract entitled Communication with Company Customer with respect to communications between Subcontractor and the Government.

1.3 AMENDMENTS REQUIRED BY PRIME CONTRACT

Subcontractor agrees that upon the request of Company it will negotiate in good faith with Company relative to amendments to this Subcontract to incorporate additional provisions herein or to change provisions hereof, as Company may reasonably deem necessary in order to comply with the provisions of the applicable Prime Subcontract or with the provisions of amendments to such Prime Subcontract. If any such amendment to this Subcontract causes an increase or decrease in the cost of, or the time required for, performance of any part of the Work under this Subcontract, an equitable adjustment shall be made pursuant to the "Changes" clause of this Subcontract.

1.4 PRESERVATION OF THE GOVERNMENT'S RIGHTS

If Company furnishes designs, drawings, special tooling, equipment, engineering data, or other technical or proprietary information (Furnished Items) which the U. S. Government owns or has the right to authorize the use of, nothing herein shall be construed to mean that Company, acting on its own behalf, may modify or limit any rights the Government may have to authorize Subcontractor's use of such Furnished Items in support of other U. S. Government prime contracts.

1.5 PROVISIONS OF THE FEDERAL ACQUISITION REGULATION (FAR) INCORPORATED BY REFERENCE

.
The following FAR clauses apply to this Subcontract and resultant Task Orders:

FAR Clause	Title	Application
FAR 52.202-1	Definitions (NOV 2013)	
FAR 52.203-3	GRATUITIES (APR 1984)	
FAR 52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)	
FAR 52.203-99	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (APR 2015)	

FAR 52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER AWARDS (OCT 2018)	(Subparagraph (d)(2) does not apply. If Subcontractor meets the thresholds specified in paragraphs (d)(3) and of the clause, (g)(2) Subcontractor shall report required executive compensation by posting the information to the Government's System for Award Management (SAM) database or to the Prime Contractor. All information posted will be available to the general public.)
FAR 52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)	(Subcontractor shall provide Company copies of any reports provided under this clause which relate to the performance of this Subcontract.)
FAR 52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT	Note 4 applies. Delete paragraph (b)(2) of the clause.)
FAR 52.215-14	INTEGRITY OF UNIT PRICES (OCT 2010)	
FAR 52.222-29	NOTIFICATION OF VISA DENIAL (APR 2015)	
FAR 52.222-50	COMBATING TRAFFICKING IN PERSONS (MAR 2015)	(Note 2 applies. In paragraph (e) Note 3 applies.)
FAR 52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION (OCT 2015)	(Applies if this Subcontract exceeds $3,500 except for commercial services are part of the purchase of a COTS item (or an item that would be a COTS item, but for minor modifications), performed by the COTS provider, and are normally for that COTS provided item. Note 8 applies.)
FAR 52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (JUN 2008)	
FAR 52.227-14	RIGHTS IN DATA - GENERAL (MAY 2014)	

FAR 52.228-3	WORKER'S COMPENSATION INSURANCE (DEFENSE BASE ACT) (JUL 2014)	(All applications must be submitted through Company to USAID's DBA Provider unless an existing policy is in force. Copy of the DBA coverage must be made available upon request).
FAR 52.233-3	PROTEST AFTER AWARD (AUG 1996)	(In the event Company's customer has directed Company to stop performance of the Work under the Prime Subcontract under which this Subcontract issued pursuant to is FAR 33.1, Company may, by written order to direct Subcontractor, Subcontractor to stop performance of the Work called for by this Subcontract. "30 days" means "20 days" in (b)(2). 1 Note paragraph applies the time first except "Government" appears in paragraph (f). In paragraph (f) add after "33.104(h) (1)" the following: "and recovers those costs from Company".)
FAR 52.242-13	BANKRUPTCY (JUL 1995)	(Notes 1 and 2 apply.)
FAR 52.242-15	STOP-WORK ORDER (AUG 1989)	(Notes 1 and 2 apply.)
FAR 52.244-5	COMPETITION IN SUBCONTRACTING (DEC 1996)	
FAR 52.244-6	SUBCONTRACTS FOR COMMERCIAL ITEMS (OCT 2018)	

FAR 52.245-1	GOVERNMENT PROPERY (JAN 2017) (ALT I) (APR 2012)	("Contracting Officer" means "DevTech" except in the definition of Property Administrator and in paragraphs (h)(1)(iii) where it is unchanged, and in paragraphs (c) and (h)(4) where it includes DevTech. "Government" is unchanged in the phrases "Government property" and "Government furnished property" and where elsewhere used except in paragraph (d)(1) where it means "DevTech" and except in paragraphs (d)(2) and (g) where the term includes DevTech. The following is added as paragraph (n) "Subcontractor shall provide to DevTech immediate notice if the Government or other customers (i) revokes its assumption of loss under any direct contracts with Subcontractor, or (ii) makes a determination that Sub contractor's property management practices are inadequate, and/or present an undue risk, or that Subcontractor has failed to take corrective action when required.")

FAR 52.249-14	EXCUSABLE DELAYS (APR 1984)	(Note 2 applies except in paragraph (a)(2); Note 1 applies to (c). In (a)(2) delete "either" and "or contractual".) (Note 2 applies except in paragraph (a)(2); Note 1 applies to (c). In (a)(2) delete "either" and "or contractual".) Under (c) add that the Prime Contractor may at its discretion choose to either extend the delivery dates or terminate the failed portion of the scope for convenience under no-cost settlement and either self-perform or subcontract the terminated scope to other sources not affected by the excusable delay.
FAR 52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT	
FAR 52.204-21	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS.	`

1.6 OTHER CLAUSES APPLICABLE TO SUBCONTRACTOR BY PRESCRIPTION IN THE PRIME CONTRACT

1.6.1 AUTHORIZED GEOGRAPHIC CODE

The authorized geographic code for procurement of goods and services under this contract is [935].

1.6.3 AIDAR 752.222-71 NONDISCRIMINATION (JUNE 2012)

a) The objectives of the 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 non-discrimination against people with disabilities; and (4) To support international advocacy for people with disabilities. The full text of USAID's policy can be found at the following Web site: http://pdf.usaid.gov/pdf_docs/PDABQ631.pdf.

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

1.6.4 AIDAR 752.222-70 USAID DISABILITY POLICY (DEC 2004)

FAR part 22 and the clauses prescribed in that part prohibit contractors performing in or recruiting from the U.S. from engaging in certain discriminatory practices.

USAID is committed to achieving and maintaining a diverse and representative workforce and a workplace free of discrimination. Based on law, Executive Order, and Agency policy, USAID prohibits discrimination in its own workplace on the basis of race, color, religion, sex (including pregnancy and gender identity), national origin, disability, age, veteran's status, sexual orientation, genetic information, marital status, parental status, political affiliation, and any other conduct that does not adversely affect the performance of the employee. USAID does not tolerate any type of discrimination (in 04/22/2016 Partial Revision 93 any form, including harassment) of any employee or applicant for employment on any of the above-described bases.

Contractors are required to comply with the non-discrimination requirements of the FAR. In addition, the Agency strongly encourages all its contractors (at all tiers) to develop and enforce non-discrimination policies consistent with USAID's approach to workplace non-discrimination as described in this clause, subject to applicable law.

1.6.6 AIDAR 752.225-70 SOURCE AND NATIONALITY WAIVER REQUIREMENTS (FEB 2012)

(a) Except as may be specifically approved by the Company's Contracting Representative, the Subcontractor must procure all commodities (e.g., equipment, materials, vehicles, supplies) and services (including commodity transportation services) in accordance with the requirements at 22 CFR Part 228 "Rules on Procurement of Commodities and Services Financed by USAID Federal Program Funds." The authorized source for procurement is Geographic Code [935]. Guidance on eligibility of specific goods or services may be obtained from the Company's Contracting Representative.
(b) Ineligible goods and services. The Subcontractor must not procure any of the following goods or services under this Subcontract:
(1) Military equipment;
(2) Surveillance equipment;
(3) Commodities and services for support of police and other law enforcement activities;
(4) Abortion equipment and services
(5) Luxury goods and gambling equipment, or
(6) Weather modification equipment.
(c) Restricted goods. The Subcontractor must obtain prior written approval of the USAID Contracting Officer through submission to the Company's Contracting Representative when procuring any of the following goods or services:
(1) Agricultural commodities;
(2) Motor vehicles;
(3) Pharmaceuticals and contraceptive items;
(4) Pesticides;
(5) Fertilizer;
(6) Used equipment; or
(7) U.S. government-owned excess property.
If the Company or USAID determines that the Subcontractor has procured any of these specific restricted goods under this Subcontract without the prior written authorization of the Company's Contracting Representative or fails to comply with required procedures under an applicable waiver as provided by the Company's Contracting Representative, and has received payment for such purposes, the Company's Contracting Representative may require the contractor to refund the entire amount of the purchase.

1.6.7 AIDAR 752.211-70 LANGUAGE AND MEASUREMENT (JUN 1992)

(a) The English language shall be used in all written communications between the parties under this Subcontract with respect to services to be rendered and with respect to all documents prepared by the contractor except as otherwise provided in the Subcontract or as authorized by the contracting officer.
(b) Wherever measurements are required or authorized, they shall be made, computed, and recorded in metric system units of measurement, unless otherwise authorized by USAID in writing when it has found that such usage is impractical or is likely to cause U.S. firms to experience significant inefficiencies or the loss of markets. Where the metric system is not the predominant standard for a particular application, measurements may be expressed in both the metric and the traditional equivalent units, provided the metric units are listed first.

1.6.8 EXECUTIVE ORDERS ON TERRORISM FINANCING

The Subcontractor is reminded that U.S. Executive Orders (including E.O. 13224) and U.S. law prohibit transactions with, and the provision of resources and support to, individuals and organizations associated with terrorism. FAR 25.701 prohibits agencies and their contractors and subcontractors from acquiring any supplies or services from individuals or organizations, if any proclamation, Executive Order, Office of Foreign Assets Control (OFAC) regulations, or statute administered by OFAC would prohibit such a transaction. Accordingly, the Contracting Officer must check the U.S. Department of the Treasury's OFAC List to ensure that the names of the Subcontractor and proposed subcontractors (and individuals from those organizations who have been made known to them), are not on the list. Mandatory FAR clause 52.225-13 Restrictions on Certain Foreign Purchases is included by reference in Section I.1 of this Contract. By accepting this Subcontract, the Subcontractor acknowledges and agrees that it is aware of the list as part of its compliance with the requirements of that clause. This provision must be included in all subcontracts/sub-awards issued under this Subcontract.

1.6.10 ORGANIZATIONAL CONFLICTS OF INTEREST: PRECLUSION FROM FURNISHING CERTAIN SERVICES AND RESTRICTION ON USE OF INFORMATION (CIB 99-17)

(a) This Subcontract may call for the Subcontractor to furnish important services in support of evaluation of Contractors or of specific activities. In accordance with the principles of FAR Subpart 9.5 and USAID policy, THE SUBONTRACTOR SHALL BE INELIGIBLE TO FURNISH, AS A PRIME OR SUBCONTRACTOR OR OTHERWISE, IMPLEMENTATION SERVICES UNDER ANY CONTRACT OR TASK ORDER THAT RESULTS IN RESPONSE TO FINDINGS, PROPOSALS, OR RECOMMENDATIONS IN AN EVALUATION REPORT WRITTEN BY THE CONTRACTOR. THIS PRECLUSION WILL APPLY TO ANY SUCH AWARDS MADE WITHIN 18 MONTHS OF USAID ACCEPTING THE REPORT, unless the Head of the Contracting Activity, in consultation with USAID's Competition Advocate, authorizes a waiver (in accordance FAR 9.503) determining that preclusion of the Subcontractor from the implementation work would not be in the Government's interest.
(b) In addition, BY ACCEPTING THIS SUBCONTRACT, THE SUBCONTRACTOR AGREES THAT IT WILL NOT USE OR MAKE AVAILABLE ANY INFORMATION OBTAINED ABOUT ANOTHER ORGANIZATION UNDER THE CONTRACT IN THE PREPARATION OF PROPOSALS OR OTHER DOCUMENTS IN RESPONSE TO ANY SOLICITATION FOR A CONTRACT OR TASK ORDER.
(c) If the Subcontractor gains access to proprietary information of other company(ies) in performing this evaluation, the Subcontractor must agree with the other company(ies) to protect their information from unauthorized use or disclosure for as long as it remains proprietary and must refrain from using the information for any purpose other than that for which it as furnished. THE SUNCONTRACTOR MUST PROVIDE A PROPERLY EXECUTED COPY OF ALL SUCH AGREEMENTS TO THE COMPANY'S CONTRACTING REPRESENTATIVE

1.6.11 AIDAR 752.209-71 ORGANIZATIONAL CONFLICTS OF INTEREST DISCOVERED AFTER AWARD (JUN 1993)

(a) The Subcontractor agrees that, if after award it discovers either an actual or potential organizational conflict of interest with respect to this Subcontract, it shall make an immediate and full disclosure in writing to the Company's Contracting Representative which shall include a description of the action(s) which the Subcontractor has taken or proposes to take to avoid, eliminate or neutralize the conflict.
(b) The Company's Contracting Representative shall provide the contractor with written instructions concerning the conflict. The Company reserves the right to terminate the Subcontract if such action is determined to be in the best interests of the Government and the Company is directed so by USAID.

1.6.12 ENVIRONMENTAL COMPLIANCE

(a) The Foreign Assistance Act of 1961, as amended, Section 117 requires that the impact of USAID's activities on the environment be considered and that USAID include environmental sustainability as a central consideration in designing and carrying out its development programs.
This mandate is codified in Federal Regulations (22 CFR 216) and in USAID's Automated Directives System (ADS) Parts 201.5.10g and 204 (http://www.usaid.gov/policy/ads/200/), which, in part, require that the potential environmental impacts of USAID-financed activities are identified prior to a final decision to proceed and that appropriate environmental safeguards are adopted for all activities. Subcontractor environmental compliance obligations under these regulations and procedures are specified in the following paragraphs of this Subcontract.
(b) In addition, the contractor must comply with host country environmental regulations unless otherwise directed in writing by Company's Contracting Representative. In case of conflict between host country and USAID regulations, the latter must govern.
(c) No activity funded under this Subcontract will be implemented unless an environmental threshold determination, as defined by 22 CFR 216, has been reached for that activity, as documented in a Request for Categorical Exclusion (RCE), Initial Environmental Examination (IEE), or Environmental Assessment (EA) duly signed by the Bureau Environmental Officer (BEO). (Hereinafter, such documents are described as "approved Regulation 216 environmental documentation.")
(d) the Company shall notify the Subcontract if specific mitigation actions are required under this clause in performance of this Subcontract.

1.6.13 COMPLIANCE WITH THE TRAFFICKING VICTIMS PROTECTION REAUTHORIZATION ACT

The company at the request of U.S. Government may terminate this Subcontract agreement, without penalty, if the Subcontractor or any subcontractor (i) engages in severe forms of trafficking in persons or has procured a commercial sex act during the period of time that the Contract is in effect, or (ii) uses forced labor in the performance of the Subcontract agreement.

1.6.14 DISCLOSURE OF INFORMATION

(a) Subcontractors are reminded that information furnished under this Subcontract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not necessarily preclude disclosure when the U.S. Office of Personnel Management (OPM or The Government) determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.
(b) Any information made available to the Subcontractor by the Government must be used only for the purpose of carrying out the provisions of this Contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the Subcontract.

(c) In performance of this Subcontract, the Subcontractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Subcontractor or the Subcontractor's responsible employees.
(d) Each officer or employee of the Subcontractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Subcontractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 19 U.S.C. 641. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine of up to $100,000, or imprisoned up to ten years, or both.

1.6.15 AIDAR 752.7034 ACKNOWLEDGEMENT AND DISCLAIMER (DEC 1991)

For use in any Subcontract which funds or partially funds publications, videos, or other information/media products.
(a) USAID shall be prominently acknowledged in all publications, videos or other information/media products funded or partially funded through this Subcontract, and the product shall state that the views expressed by the author(s) do not necessarily reflect those of USAID. Acknowledgements should identify the sponsoring USAID Office and Bureau or Mission as well as the U.S. Agency for International Development substantially as follows:
"This (publication, video or other information/media product (specify)) was made possible through support provided by the Office of ___, Bureau for ___, U.S. Agency for International Development, under the terms of Contract No. ___. The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of the U.S. Agency for International Development."
(b) Unless the Subcontractor is instructed otherwise by the Company's Contracting Representative, publications, videos or other information/media products funded under this Subcontract and intended for general readership or other general use will be marked with the USAID logo and/or U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT appearing either at the top or at the bottom of the front cover or, if more suitable, on the first inside title page for printed products, and in equivalent/appropriate location in videos or other information/media products. Logos and markings of co-sponsors or authorizing institutions should be similarly located and of similar size and appearance.

1.6.17 RESTRICTIONS AGAINST DISCLOSURE (MAY 2016)

(a) The Subcontractor agrees, in the performance of this Subcontract, to keep the information furnished by the Government or acquired/developed by the Subcontractor in performance of the contract and designated by Company's Contracting Representative, in the strictest confidence. The Subcontractor 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 Subcontractor's possession, to those employees needing such information to perform the work described herein, i.e., on a "need-to-know" basis. The Subcontractor agrees to immediately notify the Company's Contracting Representative in writing in the event that the Subcontractor determines or has reason to suspect a breach of this requirement has occurred.
(b) All Subcontractor 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 Subcontractor 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 Subcontract.

1.6.18 MEDIA AND INFORMATION HANDLING AND PROTECTION (MAY 2016)

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

(c) Handling and Protection. The Subcontractor is responsible for the proper handling and protection of Sensitive Information to prevent unauthorized disclosure. Within 45 calendar days of the award, the Subcontractor must develop 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 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 Subcontract, the Subcontractor must return all Agency records and media provided by USAID and/or obtained by the Subcontractor 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 Subcontractor must execute secure destruction (either by the Subcontractor 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 Subcontractor 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 Subcontractor shall include the substance of this special contract requirement in all subcontracts, including this paragraph (f).

1.6.19 PRIVACY AND SECURITY INFORMATION TECHNOLOGY SYSTEMS INCIDENT REPORTING (MAY 2016)

(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 and Privacy Incident” means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
(b) This special contract requirement applies to the Subcontractor and all personnel providing support under this Subcontract (hereafter referred to collectively as “Subcontractor”) and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), E-Government Act of 2002 - Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.
(c) Privacy Act Compliance
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 Subcontractor personnel must complete USAID-provided mandatory security and privacy training prior to gaining access to USAID information systems and annually thereafter.
(2) The USAID Rules of Behavior must be signed by each user prior to gaining access to USAID information systems, periodically at the request of USAID, or whenever the Rules are updated. 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) Subcontractor employees filling roles identified by USAID as having significant security responsibilities must complete role-based training upon assignment of duties and thereafter at a minimum of every three years.
(5) Within fifteen (15) calendar days of completing the initial IT security training, the Subcontractor must notify the Company’s Contracting Representative in writing that its employees, in performance of the contract, have completed the training. The Company’s Contracting Representative will inform the contractor of any other training requirements.
(e) Information Security and Privacy Incidents
(1) Security Incident Reporting Requirements: All Information Security Incidents must be reported in accordance with the requirements below, even if it is believed that the Incident may be limited, small, or insignificant. USAID will determine the magnitude and resulting actions.
i. Subcontractor employees must report all Information Security Incidents to the USAID Service Desk immediately, but not later than 30 minutes, after becoming aware of the Incident, at: CIO-HELPDESK@usaid.gov, (202) 712-1234, regardless of day or time, as well as the Subcontractor Facilities Security Officer. Subcontractor employees are strictly prohibited from including any Sensitive Information in the subject or body of any e-mail. To transmit Sensitive Information, Subcontractor employees must use FIPS 140-2 compliant encryption methods to protect Sensitive Information in attachments to email. Passwords must not be communicated in the same email as the attachment.
ii. The Subcontractor must provide any supplementary information or reports related to a previously reported incident directly to 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 Incident Reporting Requirements: USAID must manage in accordance with Federal laws and regulations the information it collects, uses, maintains, and disseminates in support of its mission and business functions. Any unauthorized use, disclosure, or loss of such information can result in the loss of

the public's trust and confidence in the Agency's ability to protect it properly. PII breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. Therefore, incidents involving a breach of PII have a critical time-period for reporting. Subcontractor and Subcontractor staff must report immediately upon discovery all potential and actual privacy breaches to the Company's Contracting Representative, the USAID Service Desk at 202-712-1234 or CIO-HELPDESK@usaid.gov, and the Privacy Office at privacy@usaid.gov, regardless of the format of the PII (oral, paper, or electronic) or the manner in which the incidents might have occurred. The subject line shall read "Action Required: Potential Privacy Incident".
(3) Incident Response Requirements
i. All determinations related to Information Security and Privacy Incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made by authorized USAID officials at USAID's discretion.
ii. The Subcontractor and contractor employees must provide full access and cooperation for all activities determined by USAID to be required to ensure an effective Incident Response, including providing all requested images, log files, and event information to facilitate rapid resolution of Information Security and Privacy Incidents.
iii. Incident Response activities required by USAID may include but are not limited to, inspections; investigations; forensic reviews; data analyses and processing; and final determinations of responsibility for the Incident and/or liability for any additional Response activities.
iv. At its discretion, USAID may obtain the assistance of Federal agencies and/or third party firms to aid in Incident Response activities.
v. When an incident is determined to be caused by the Subcontractor or the contractor's employees through neglect or purposeful conduct, the Subcontractor must be responsible for all costs and related resource allocations required for all subsequent Incident Response activities determined to be required by USAID, whether incurred by USAID, agents under contract or on assignment to USAID, or by third party firms.
(f) The Subcontractor 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 Subcontractor is required to include the substance of this provision in any subcontracts that require the subcontractor, subcontractor employee, or consultant to design, development, or operation of a System of Records on individuals to accomplish an agency function.
In altering this special contract requirement, require subcontractors to report information security and privacy incidents directly to at the USAID Service Desk at 202-712-1234 or CIOHELPDESK@ usaid.gov/ and the Privacy Office at privacy@usaid.gov. A copy of the correspondence shall be sent to the prime Subcontractor (or higher tier subcontractor) and the Contracting Officer referencing the ticket number.

1.6.20 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION RESOURCES (APRIL 2018)

(a) Definitions. As used in this special contract requirement-
"Audit Review" means the audit and assessment of an information system to evaluate the adequacy of implemented security controls, assure that they are functioning properly, identify vulnerabilities and methods for mitigating them and assist in implementation of new security controls where required. These reviews are conducted periodically but at least annually, and may be performed by USAID Bureau for Management, Office of the Chief Information Officer (M/CIO) or designated independent assessors/auditors, USAID Office of Inspector General (OIG) as well as external governing bodies such as the Government Accountability Office (GAO).
"Authorizing Official" means the authorizing official is a senior government official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and/or the Nation.

“Information” means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
“Sensitive” Information or Sensitive But Unclassified (SBU) - Sensitive But Unclassified (SBU) describes information which warrants a degree of protection and administrative control and meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act, 12 FAM 540 Sensitive but Unclassified Information (TL;DS-61;10-01-199), and 12 FAM 541 Scope (TL;DS46;05-26-1995). SBU information includes, but is not limited to: 1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to an individual or group, or could have a negative impact upon foreign policy or relations; and 2) Information offered under conditions of confidentiality, arising in the course of a deliberative process (or a civil discovery process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers.
“National Security Information” means information that has been determined pursuant to Executive Order 13526 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified or national security information is specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.
“Information Technology Resources” means agency budgetary resources, personnel, equipment, facilities, or services that are primarily used in the management, operation, acquisition, disposition, and transformation, or other activity related to the lifecycle of information technology; acquisitions or interagency agreements that include information technology and the services or equipment provided by such acquisitions or interagency agreements; but does not include grants to third parties which establish or support information technology not operated directly by the Federal Government. (OMB M-15-14)
(b) Applicability: This special contract requirement applies to the Subcontractor, its subcontractors, and all personnel providing support under this contract (hereafter referred to collectively as “Contractor”) and addresses specific USAID requirements in addition to those included in the Federal Acquisition Regulation (FAR), Privacy Act of 1974 (5 U.S.C. 552a - the Act), EGovernment Act of 2002 – Section 208 and Title III, Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), the Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) and the 800-Series Special Publications (SP), Office of Management and Budget (OMB) memorandums, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data.
(c) 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 Prime Contractor, 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 Prime Contractor, in consultation with the USAID.

(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 through the Prime Contractor. 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 Prime Contractor.

(iv) Prior to the Agency security assessment, authorization and approval, the Contractor must coordinate with the Prime Contractor and designated 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. Submissions must be made with copy to the Prime Contractor.

(vii) USAID retains the right to deny or rescind the ATO for any system if it believes the package or system fails to meet the USAID security requirements. Moreover, USAID may or may not provide general or detailed guidance to the Contractor to improve the SA&A package or the overall security posture of the information system and may or may not

require re-submission of the package upon completion of the modifications. USAID reserves the right to limit the number of resubmissions at its convenience and may determine a system's compliance to be insufficient at which time a final determination will be made to authorize or deny operation. USAID is the final authority on the compliance.
(viii) The Contractor must submit SA&A packages to the CIO at least sixty (60) days prior to production or the expiration of the current ATO.
(ix) Once the USAID Chief Information Security Officer or designee determines the risks, the Contractor must ensure that all Plan of Action and Milestones resulting from security assessments and continuous monitoring are remediated within a time frame commensurate with the level of risk as follows:

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

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

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

1.6.21 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 Subcontractor 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, Federal information shall only be for purposes specified in this contract.

(ii) The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

(iii) These access, use, and disclosure prohibitions and obligations shall remain effective beyond the expiration or termination of this contract.

(2) The Contractor shall use related Federal information only to manage the operational environment that supports the Federal information and for no other purpose unless otherwise permitted with the prior written approval of the Prime Contractor.

(d) Records Management and Access to Information

(1) The Contractor shall support a system in accordance with the requirement for Federal agencies to manage their electronic records in accordance with capabilities such as those identified in the provisions of this contract and National Archives and Records Administration (NARA) retention policies.

(2) Upon request by the government, the Contractor shall deliver to the Prime Contractor all Federal information, including data schemas, metadata, and other associated data artifacts, in the format specified in the schedule or by the Prime Contractor 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 Federal information in accordance with records retention provisions negotiated by the terms of the contract and in accordance with USAID records retention policies.
(4) The Contractor shall dispose of Federal information in accordance with the terms of the contract and provide the confirmation of disposition to the Prime Contractor in accordance with contract closeout procedures.

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

(f) Spillage and Information Security Incidents: Upon written notification by the Government of a spillage or information security incident involving classified information, or the Contractor's discovery of a spillage or security incident involving classified information, the Contractor shall immediately (within 30 minutes) notify CIO-HELPDESK@usaid.gov and the Office of Security at SECinformationsecurity@usaid.gov to correct the spillage or information security incident incompliance with agency-specific instructions. The Contractor will also notify the Prime Contractor. The Contractor will abide by Prime Contractor or 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 Prime Contractor. 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: CIOHELPDESK@usaid.gov, regardless of day or time, as well as the Prime Contractor. 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 nonproprietary format that USAID requests at the time of production, unless the parties agree otherwise.

(j) Security Requirements:

(1) The Contractor shall adopt and maintain administrative, technical, operational, and physical safeguards and controls that meet or exceed requirements contained within the Federal Risk and Authorization Management Program (FedRAMP) Cloud Computing Security Requirements Baseline, current standard for NIST 800-53 (Security and Privacy Controls for Federal Information Systems) and Organizations, including Appendix J, and FedRAMP Continuous Monitoring Requirements for the security level and services being provided, in accordance with the security categorization or impact level as defined by the government based on the Federal Information Processing Standard (FIPS) Publication 199 (FIPS-199).

(2) The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the security assessment and authorization (SA&A) is based on the system's complexity and security categorization. The Contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at https://www.FedRAMP.gov.

(3) The Contractor must support SA&A activities to include assessment by an accredited Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan. The Contractor must make available to the Contracting Officer, the most current, and any other, Security Assessment Reports for consideration as part of the Contractor's overall Systems Security Plan.

(4) The Government reserves the right to perform penetration testing or request Penetration Testing by an independent source. If the Government exercises this right, the Contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include but are not limited to scanning operating systems, web applications, databases, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Federal information for vulnerabilities.

(5) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the Contractor's implementation as documented in the Security Assessment Report must be tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before any restricted authorization is issued.

(6) The Contractor is responsible for mitigating all security risks found during SA&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within thirty (30) calendar days and all moderate risk vulnerabilities must be mitigated within sixty (60) calendar days from the date vulnerabilities are formally identified. USAID may revoke an ATO for any system if it is determined that the system does not comply with USAID standards or presents an unacceptable risk to the Agency. The Government will determine the risk rating of vulnerabilities.

(7) The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements and to allow for appropriate risk decisions for an Information Technology security program. The Government reserves the right to conduct onsite inspections. The Contractor must make appropriate personnel available for interviews and provide all necessary documentation during this review and as necessary for continuous monitoring activities.

(k) Privacy Requirements: Cloud Service Provider (CSP) must understand and adhere to applicable federal Privacy laws, standards, and guidance to protect Personally Identifiable Information (PII) about individuals that will be collected and maintained by the Contractor solution. The Contractor responsibilities include full cooperation for any request for disclosure, subpoena, or other judicial process seeking access to records subject to the Privacy Act of 1974.

(l) Data Location: The Contractor must disclose the data server locations where the Agency data will be stored as well as the redundant server locations. The Contractor must have prior Agency approval to store Agency data in locations outside of the United States.

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

(n) Service Level Agreements (SLAs): The Contractor must be willing to negotiate service levels with USAID; clearly define how performance is guaranteed (such as response time resolution/mitigation time, availability, etc.); monitor their service levels; provide timely notification of a failure to meet the SLAs; and evidence that problems have been resolved or mitigated. Additionally, at the Prime Contractor or 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. The Prime Contractor or 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 the Prime Contractor and 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

1.6.22 SKILLS AND CERTIFICATION REQUIREMENTS FOR PRIVACY AND SECURITY STAFF (MAY 2016)

(a) Applicability: This special contract requirements applies to the Subcontractor, its subcontractors and personnel providing support under this contract and addresses the Privacy Act of 1974 (5 U.S.C. 552a - the Act) and Federal Information Security Management Act (FISMA) of 2002 (FISMA, Public Law 107-347. 44 U.S.C. 3531-3536).
(b) Subcontractor employees filling the role of Information System Security Officer and Information Security Specialists must possess a Certified Information Systems Security Professional (CISSP)

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

This will fulfill the requirements for specialized training due to the continuing education requirements for the certification. Subcontractor employees must provide proof of their certification status upon request.

1.6.23 PROHIBITION OF ASSISTANCE TO DRUG TRAFFICKERS

The Company at the direction of USAID reserves the right to terminate this contract, to demand a refund or take other appropriate measures, if the subcontractor has been convicted of a narcotics offence or to has been engaged in drug trafficking as defined in 22 CFR Part 140.

1.6.248 FAR 52.223-99 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS (OCT 2021)

(a) Definition. As used in this clause - United States or its outlying areas means—

(1) The fifty States;
(2) The District of Columbia;
(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;
(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and
(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).

(c) Compliance. The Subcontractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this subcontract, for contractor or subcontractor workplaces published by the Safer Federal Workforce Task Force (Task Force Guidance) at https://www.saferfederalworkforce.gov/contractors/. While at a Prime Contractor (Palladium) or U.S. Government workplace, covered subcontractor employees must also comply with any additional Prime Contractor or agency workplace safety requirements for that workplace that are applicable to federal employees, as amended (see USAID’s COVID-19 Safety Plan and Workplace Guidelines (Safety Plan)).

(d) Subcontracts. The Subcontractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part in the United States or its outlying areas.

(End of clause)

Date of Offer:

Name of Offeror:

Typed Name and Title:

Signature_____Date:

DEVTECH
Innovative Solutions for Development

ANNEX C

Certification Regarding Debarment, Suspension, or Proposed Debarment

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

Vendor Name: _____

Signatures: _____

Signatory Name: _____

Signatory Title: _____

Date: _____

DEVTECH
Innovative Solutions for Development

ANNEX D

Information Concerning Work-Day, Work-Week, & Paid Absences -

(Add a paragraph with brief description on your general policies)

The normal work periods are:

PERIOD	NORMAL WORK HOURS
Work-day	Add #hours
Work-week	Add #hours
Work-year	Add #hours
Work-week for temporary duty travel for short-trips (paid at regular rate)	Add #hours

Please explain how all paid absences are recovered.

- Vacation: Employees are granted (add #days) days of vacation leave during their first year and one additional day per year.
- Holidays: Employees are granted (add # days) days of federal holidays. Employees based in an overseas office are granted holidays in accordance with the holiday established by the host country government.
- Sick/Personal Leave: Employees are granted (add # days) days of personal leave each year.
- Add others as applicable

ANNEX E

See attached excel template (click hyperlink to access the file)