The USAID Laos Business Environment Activity (LBE)

In collaboration with

Digital Frontiers' Digital Asia Accelerator (DAA)

Request for Applications (RFA)

No. 2023-05

Accelerator IT Security and Cybersecurity Training Services in Laos

Issue Date: September 8, 2023

Key Dates of RFA #2023-05, "Accelerator IT Security and Cybersecurity Training Services in Laos," issued on September 8, 2023

A Virtual Applicants Conference will be held on September 22, 2023 (10:00AM – 11:30AM Laos time) where you can learn more about this opportunity.

Please join us via this link!

Virtual applicants conference Q&A:	September 22, 2023 (10:00AM Laos)
Deadline to submit applications:	October 6, 2023 (5:00PM Laos)
Where to submit questions & applications:	email only to DAA_subawards@dai.com

DAA_subawards@dai.com is the sole point of contact for this RFA.

Any prospective applicant who fails to confirm their interest with DAA_subawards@dai.com assumes complete responsibility if they do not receive direct communications (amendments, answers to questions, etc.) prior to the RFA closing date.

Summary of RFA 2023-05: Accelerator IT Security and Cybersecurity Training Services in Laos

Purpose: What is being funded?

The USAID Laos Business Environment Activity (LBE), in collaboration with DAI, through USAID's Digital Asia Accelerator program (DAA), seeks a qualified organization ("the provider") in Laos to deliver DAA's "Accelerator IT Security and Cybersecurity Training" to private sector businesses in Laos. Trainings will be delivered in-person and in the Lao language. The overall goal of this effort is to increase awareness, skills and knowledge in cybersecurity control measures and best practices for private sector businesses in Laos.

Anticipated Award Value (in USD)

LBE and DAA anticipates awarding one (1) grant with a budget between $30,000-$50,000.

Eligibility: who can apply?

Applicants must meet the following minimum requirements to apply:

- Location: You must have a physical presence in Laos;
- You must be fully registered to legally operate in Laos;
- Possess relevant in-country experience, background and expertise to assist participants in the topic of cybersecurity.
- Per US federal regulation, application budgets should capture all costs of the activity (salaries, purchases, rentals, office support costs, etc.). Application budgets should not include additional fees that would lead to the grantee making a profit. Profit is defined as any amount in excess of the cost of the activity;
- Government entities and individuals are not eligible;
- Language: Applications must be submitted in English;
- There is a **mandatory** requirement for your organization to be fully registered on SAM.gov, with the accompanying UEI and CAGE/NCAGE numbers. For detailed information on registration in the above USG databases, see Attachment D - Instructions for Obtaining CAGE/NCAGE Code, SAM Registration, and UEI.

Organizations must submit a written application to be considered for award. What must applications include to be considered for award?

1. **A technical application (10 pages max) which includes:**

   - **Narrative technical approach** outlining how you will implement the program;
   - Your **organizational capacity and experience** to implement the program;
   - Your **experience and knowledge** of IT security and cybersecurity concerns in Laos.

2. **A workplan** (in Gantt chart format) to demonstrate your ability to complete the program within three months. The workplan detailed activity timelines and key milestones.

3. **A staffing plan (2 pages max)** that includes titles and job responsibilities of your proposed team. The personnel plan must:
   - demonstrate an effective management and coordination plan for proposed personnel, and;
   - include short bios for the top three team members (1-page bio maximum for each team member).

4. **CVs of proposed personnel**. Each CV should not exceed 3 pages.

5. **A Past Performance Matrix** (see **Attachment B** for format) containing three relevant past performance examples preferably including any IT security and cybersecurity training projects conducted in Laos or elsewhere.

6. **A Budget** ($30,000 - $50,000 USD max) See **Attachment A** for budget format. The budget must:
   - Reflect accurate, reasonable local market prices;
   - Include all costs, with as much detail as possible;
   - Confirm that applicant is responsible for all applicable taxes and fees;
   - Be fully compliant with local labor and financial regulation.

7. **A Budget Narrative** to explain the budget. See **Attachment A** for Narrative format. The Narrative must:
   - Explain and justify each budget line;
   - Provide enough unit price detail to allow DAI to confirm budgeted prices are reasonable for the Laos market;
   - Submit Proof of Registration in Laos.
   - Complete the Financial Capacity Questionnaire (Attachment F), to confirm your capacity to manage grant funds.

Program Description: Accelerator IT Security and Cybersecurity Training Services in Laos

Objective

LBE and DAI are searching for a training provider in Laos to deliver the Accelerator IT Security and Cybersecurity training to private sector businesses in Laos. Trainings will be delivered in-person and in the Lao language. The overall goal of this effort is to increase awareness, skills and knowledge in cybersecurity control measures and best practices for private sector businesses in Laos.

Note that DAA has already developed the training materials, which are in PowerPoint slide format. The selected training provider will be responsible for delivering the training using the developed training materials. The training materials will be shared with the selected training provider during grant award negotiations. The training materials will be translated into Lao language by LBE.

Location

The Accelerator IT Security and Cybersecurity Training Course will take place in Laos.

Period of Performance

The activity will run for approximately 3 - 5 months, with target starting date in November 2023 and concluding in March 2024.

Background

The USAID Laos Business Environment Activity (LBE), in collaboration with DAI, through USAID's Digital Asia Accelerator program (DAA) is looking to provide support to SMEs to strengthen their cybersecurity knowledge and digitals skills. DAA, managed by DAI, aims to increase the safe and appropriate use of digital technology for economic development in Southeast Asia and Mongolia [1] . LBE, managed by International Business Initiatives (IBI), aims to enhance the competitiveness of MSMEs while strengthening the business environment in Laos.

To help achieve LBE and DAA objectives, DAI seeks a qualified service provider ("the provider") to deliver DAA's "Accelerator IT Security and Cybersecurity Training" to private sector businesses in Laos to increase awareness, skills and knowledge in cybersecurity control measures and best practices.

Due to the pandemic, businesses have rapidly adapted to remote and hybrid work models, while becoming increasingly dependent on the internet to remain competitive and reach customers. Digital transformation in emerging markets such as Laos continue to play a key role in economic growth as it helps enable trade, cashless payments and efficient delivery of products and services.[2] With the digital economy in Southeast Asia expected to more than double in size from $170bn in 2021 to $360bn by 2025, then to $1tn by 2030[3], internet adoption in Laos continues to surge, driven by an increase in mobile phone usage, reaching more than 98% of the population with approximately one million subscribed to mobile banking.[4] However, due to widespread use of internet technology, businesses have become attractive targets for cybercrimes, as most are considerably unprepared and unaware of how to protect data, with many not knowing the extent of damage cyberattacks can cause.[5]

Given this, the Accelerator has identified the need for businesses in Laos to improve their skills in IT security and cybersecurity. While internet technology has become more accessible in the country, businesses lack knowledge in cybersecurity, making businesses vulnerable to cyberattacks, raising the urgency in the need to raise awareness about data security and potential impact of cyberattacks on businesses and the people that it serves. The topic of cybersecurity is now of high importance for businesses to avoid potential breaches, attacks, and risks for cyberattacks. Additionally, there are added business benefits to IT security and cybersecurity, including maintaining customer trust, protecting business reputation, and improving data management, business efficiency, and access controls and accountability.

The Accelerator SME IT Security and Cybersecurity Training was first delivered virtually in September 2022 in collaboration with the USAID Responsible Investment and Trade Activity (RITA) in Myanmar. DAA and RITA delivered the SME IT security and cybersecurity training to 36 Myanmar companies to date and continues to deliver virtual trainings to subsequent cohorts through 2025. The training resulted in increased knowledge in IT security and cybersecurity, as well as improved ability to adopt and implement cybersecurity control measures and best practices into day-to-day business operations. Given the

[1] DAA is part of a broader DAI-managed project, Digital Frontiers, which works closely with the U.S. Global Development Lab, the Center for Digital Development, USAID missions, the private sector, and international and local development organizations to identify successful and sustainable digital approaches and scale their impact globally.

[2] The World Bank. 2022. "Positioning the Lao PDR for a digital future."

[3] The Business Times. 2022. "Amid greater digitalisation, SMEs must contend with issues such as cyber attacks and finding talent: panel." https://www.businesstimes.com.sg/international/amid-greater-digitalisation-smes-must-contend-issues-such-cyber-attacks-and-finding

[4] The World Bank. 2022. "Positioning the Lao PDR for a digital future."

[5] Techwire Asia. 2021. "Cybersecurity is still challenging for ASEAN businesses." https://techwireasia.com/2021/11/cybersecurity-are-challenging-asean-businesses/

success of the trainings in Myanmar, DAA seeks to deliver the training curriculum through in-person training in Laos in partnership with a Lao-based training provider or IT service provider. Below are the topics covered in the training:

- Module 1: Be aware of cybersecurity threats.
- Module 2: Use a strong password.
- Module 3: Enable multi-factor authentication (MFA).
- Module 4: Understanding VPN.
- Module 5: Use antivirus software.
- Module 6: Configure security settings.
- Module 7: Back up critical data regularly.
- Module 8: Minimize use of public WIFI.
- Module 9: Use genuine software.
- Module 10: Keep software updated.
- Module 11: Password protect files before emailing.
- Module 12: Know your IT assets.

Applicants are free to propose additional modules that it deems critical in Laos.

As stated above under the Objective, note that DAA has already developed the training materials, which are in PowerPoint slide format. The selected training provider will be responsible for delivering the training using the developed training materials, which are approximately 230 PowerPoint slides covering 12 modules. The training materials PowerPoint slides will be shared with the selected training provider during grant award negotiations.

Target activities/outcomes: The provider shall deliver the following activities and outcomes.

1. Deliver training Work Plan, Timeline, Responsibilities and other training details.

The provider will deliver the training work plan, timeline and responsibilities, which will be reviewed and agreed upon by the Accelerator and LBE. Proposals for formats and methods on how best to incentivize and deliver the training to ensure maximum level of content retention for participants will also be reviewed. The provider will also provide a team of experienced training and IT experts to deliver the training. Please refer to the qualifications below. The provider should have the following qualifications:

1. Instructor/experts must have relevant background, expertise and experience to assist participants in the topic of cybersecurity.
2. Provider must possess relevant in-country experience and have physical presence in-country.
3. Provider must have documented ability to meet required delivery timelines, as demonstrated through at least three (3) reference letters from prior clients.
4. Provider may have the potential to be the platform to build a network to connect global and regional cybersecurity peers and experts through live events, learning seminars, and community.

Also, DAA prefers that instructors/experts possess relevant internationally recognized professional certifications including inter alia, OSCP, eJPT, eWPT, eCXD, and/or eMAPT.

2. Prepare the agenda and review course materials

The provider will prepare the training agenda and review the course materials in both English and Lao language, and provide any input and comments to improve content and delivery. The course would be one full day or two half-day[6] in-person sessions covering the cybersecurity topics with certification provided upon successful completion of the course. The course should include short assessments at the beginning and end of the training to assess the participants' understanding and retention of the topics covered. The provider will require participants to complete and pass the final assessment to hold participants accountable for their learning.

3. Prepare marketing and registration materials for the training

The provider will be responsible for preparing marketing materials which will include relevant information on the training such as date, time, place, language, agenda, how to register, etc. Proposals for marketing collaterals such as banner and backdrop and registration formats and methods to reach beneficiaries and to ensure high level of participation and engagement in the training will be reviewed and agreed upon by the Accelerator and LBE.

4. Select and register participants for the training

[6] The number of sessions and the duration of each session will be determined once a service provider is chosen. These decisions will be made on a case-by-case basis for each location.

The provider will share the selection criteria for the training which will be reviewed and agreed upon by the Accelerator and LBE. Information on the training with specific information about registration, as well as clear value proposition for participants and companies will be compiled by the provider to be shared by email to potential participants.

5. Deliver at least 4 in-person training sessions to businesses in Laos

The provider will deliver at least 4 training sessions (each session will be either one full day or two half-day, in-person sessions). Each training session should have at least 30 to 50 participants and will be delivered in the Lao language. The provider will issue a certificate to participants who complete the course and pass the final assessment. The provider shall also submit a copy of the certificate to the Accelerator as documented evidence of course completion.

6. Submit final report

The provider will submit a final report detailing the objectives, methodology, participant list, evaluation results including feedback. The report should also include photos from the training, participant quotes, lessons learned and recommendations.

Evaluation of Applications: How will the winner be selected?

All applications that meet the application requirements will be reviewed by a review panel made up of LBE and DAA personnel.

The applications will be evaluated according to the evaluation criteria set forth below. To the extent necessary (if an award is not made based on initial applications), negotiations may be conducted with each applicant whose application, after discussion and negotiation, has a reasonable chance of being selected for the award. **Award will be made to responsible applicants whose applications offer the best value**.

LBE and DAA will review all eligible applications, and make an award based on the technical and cost evaluation considerations stated above and select the application that provides the best value to LBE and DAA. LBE and DAA may also exclude an application from consideration if it determines that an Applicant is "not responsible", i.e., that it does not have the management and financial capabilities required to perform the work required.

Evaluation points will not be awarded for cost. Cost will primarily be evaluated for realism and reasonableness. LBE and DAA may award to a higher priced applicant if a determination is made that the higher technical evaluation of that applicant merits the additional cost/price. Similarly, LBE and DAA may reject an application with the highest technical evaluation in favor of a favorably priced offer. LBE and DAA strongly recommend that applicants' initial applications represent their best value.

Awards will be made based on the ranking of applications by the review panel according to the evaluation criteria and scoring system identified below:

No.	Evaluation Criteria	Maximum Points
1.	Application provides clear activity summary, objectives and explanation on how the proposed technical approach will increase awareness, skills and knowledge in cybersecurity control measures and best practices for private sector businesses in Laos.	10 points
2.	Application demonstrates understanding of problems addressed, solutions delivered and target beneficiary group(s), including: a) gaps that need to be addressed in the topic of IT security and Cybersecurity for businesses in Laos; b) thorough understanding of topics covered in the training (see page 5) and how the training addresses the needs; c) clear definition of the target beneficiaries and their interests, capabilities and needs; d) clear explanation of formats/methods on how best to incentivize and deliver the training to ensure maximum level of content retention for participants; e) clear explanation of formats/methods used for marketing, implementation and registration to reach beneficiaries to ensure high level of participation and engagement in the training; f) if able, present ideas for a platform to build a network to connect global and regional cybersecurity peers and experts through live events, learning seminars, and community.	30 points
3.	Technical approach is implementable within the proposed timeframe and budget.	10 points
4.	Application specifies the project's target results and outcomes, and how those results and outcomes will be measured.	10 points
5.	Application includes a viable argument for how this activity can be sustainable after the award or deliver sustainable impact.	10 points
6.	Key personnel and training staff proposed have the relevant skills and experience to implement proposed activity.	15 points
7.	Application includes summary descriptions of at least three of the applicant's relevant past projects that demonstrate the core capabilities required to execute the proposed project.	15 points
Total Points		100 points

Attachment A: Budget and Budget Narrative Template

	Name	Rate	Units (month/day/hour)	Cost
I. Salaries and Wages				
Person 1	TBD	$0.00	0	$0
Person 2	TBD	$0.00	0	$0
Total Salaries and Wages			0	$0
II. Travel, Transportation and Per Diem				
1. Air Travel				
International Travel		$0.00	0	$0
Regional / In-Country Travel		$0.00	0	$0
2. Per Diem				
Traveler 1		$0.00	0	$0
3. Other Travel Expenses				
Traveler 1		$0.00	0	$0
Total Travel, Transportation and Per Diem				$0
III. Other Direct Costs				
1. Project Management Expenses				
Other (DESCRIBE)		$0.00	0	$0
Total Other Direct Costs				$0
Total Program Expenses				$0
Indirect Costs on All Costs			0	$0
Grand Total				$0

Budget Narrative Template

Salaries and Wages
For our labor cost estimates, we have used daily rates per person as supported by actual salaries and/or prevailing labor rates. If labor is based on commercial rates, please provide a link or evidence of publication of the commercial rates.

Personnel

- Name, Title proposed for a total of XX days at a daily rate of $XXX.
- Name, Title proposed for a total of XX days at a daily rate of $XXX.

Travel, Transportation and Per Diem
Economy air fare trips have been budgeted from XXXX to XXXX.

Regional / In-Country Travel
X number of trips have been budgeted for X locations.

Per Diem
Per Diem at $XXX has been assumed for all travelers to XXX based on XX days per trip.

Miscellaneous Travel Expenses
Miscellaneous Travel expenses of $XXX per trip have been budgeted based on the number of international trips. This cost per trip is based on XX assumptions.

Other Direct Costs
This category includes basic support costs for the project. Included within this cost category are all costs necessary for the successful operation of this activity.

Indirect Costs on All Costs
All indirect costs must be in accordance with the organization’s policies. Per 2 CFR 700.13, profit must be excluded from cost applications.

Attachment B: Past Performance Table Template

Applicants must demonstrate relevant working experience in Laos and include summary descriptions of three relevant projects that demonstrate experience, background and expertise in delivering training, particularly in the topic of cybersecurity. Applicants should include details with hyperlinks to more information if necessary. Projects should have been undertaken in the past three years. Projects undertaken in the past six years may be taken into consideration at the discretion of the evaluation committee.

#	Project Title	Project Activities	Reference(s) Name, email and/or phone	Donor / Client	Project Budget (USD)	Start & End Dates	Any Problem(s) Encountered and Resolved

Attachment C: Application Checklist

Before submitting your application, please check to make sure the following are included:

□ Application (no more than 15 pages)
□ Application contains Workplan
□ Application contains Staffing Plan
□ CVs of named team members (maximum 3 pages each)
□ Past Project Examples (Attachment B)
□ Budget
□ Budget narrative
□ Completed Financial Capability Questionnaire
□ NICRA or Audited Financial Reports, if application
□ Incorporation Papers or Certificate of Registration and Statute
□ Personnel, procurement, and finance manuals

Attachment D: Instructions for Obtaining a CAGE/NCAGE Code, SAM Registration, and UEI

Background: Summary of Current U.S. Government Requirements

There are mandatory requirements for grantees to obtain the following items/registration before an award of any kind can be issued. Without registering in the required databases, DAA cannot deem an Applicant to be "responsible" to conduct business with and therefore, DAI will not enter into an agreement with any such organization. The award of a grant resulting from this RFA is contingent upon the winner providing a UEI, a CAGE/NCAGE code, and proof of registration in the SAM.gov system. Organizations who fail to provide these will not receive an agreement and DAI will select an alternate Applicant.

CAGE/NCAGE Code

The Commercial and Government Entity (CAGE) Code was established by the US. The NATO Codification System developed the NATO Commercial and Government Entity (NCAGE) Code. When a business/organization is assigned a CAGE/NCAGE, they are in fact the same type/structure of code but identifies which nation or if the NATO Support Agency assigned the CAGE/NCAGE. You must have a CAGE/NCAGE code before registering in SAM.

- Link to the CAGE/NCAGE Code request: https://eportal.nspa.nato.int/AC135Public/scage/CageList.aspx
- Link to CAGE/NCAGE code request instructions: https://eportal.nspa.nato.int/AC135Public/Docs/US%20Instructions%20for%20NSPA%2 0NCAGE.pdf

System for Award Management (SAM) Registration

You must have an active registration with www.SAM.gov to do business with the Federal Government. To register in SAM, at a minimum, you will need the following information:

- U.S. Registrants:
  1) Your Legal Business Name and Physical Address
  2) Your Taxpayer Identification Number (TIN) and Taxpayer Name associated with your TIN; Review your tax documents from the IRS (such as a 1099 or W-2 form) to find your Taxpayer Name
  3) Your bank's routing number, your bank account number, and your bank account type, i.e. checking or savings, to set up Electronic Funds Transfer (EFT)
- International Registrants:
  1) Your NATO Commercial and Government Entity (NCAGE) Code

Follow this link to create a Sam.gov user account and register your organization: https://sam.gov/content/entity-registration

Unique Entity ID (UEI)

On April 4, 2022, the federal government transitioned away from the DUNS Number to the new Unique Entity ID (SAM), or 'UEI,' for entity identification of federal awards government-wide. Entity identification in federal awards (grants, loans, contracts, etc.) means a unique set of numbers and letters used to identify every entity seeking to do business with the federal government. Currently, and through April 3, 2022, the federal government uses the DUNS Number, assigned by Dun & Bradstreet. On April 4, 2022 and moving forward, the federal government will use the Unique Entity ID (SAM), or "UEI" assigned by SAM.gov.

For new entities:

- Prior to starting entity validation process, an entity should be prepared with documents that: (1) shows the entity's legal business name and physical address in the same document and is less than 5 years old; (2) shows the legal business name and start year in the same document; and, (3) shows legal business name and US state of Incorporation (for US entities) or National Identifier (for non-US entities). If any documents are in a language other than English, they must be accompanied by certified translations (see the link below for more details).
- This GSA guide has detail on documentation requirements. It includes a downloadable document outlining what type of documentation is acceptable, general guidelines, and guidance on translations.
- Additionally there is a general FAQ also maintained by GSA.

If, after entering the required information, an entity receives a validation error message and/or is not a match with any of the returned potential matches, the entity should create an incident. There are two new, useful videos that GSA has recently published to help explain this process. These are different than the brief overview video that has been previously shared, so projects and partners are encouraged to watch:

- This video provides a detailed, step-by-step walk through of the entity validation process. Be advised the scenario it addresses is for an existing entity that has to update some information (rather than a new entity, which is the case for most of our partners), but the steps are the same: https://www.youtube.com/watch?v=ZKc9UfxtOIA (the "create incident portion" runs from 27:58 to 35:05).
- This video provides guidance on how to manage the validation ticket once it has been submitted: https://www.youtube.com/watch?v=a3nPZvnPpE0 (the "managing your validation ticket" portion runs from 17:34 to 28:55).

Entities need to regularly check their email – including spam folders – after they have submitted the incident report for emails from fsdsupport@gsa.gov. They should be able to look up the status either by logging into their user account on SAM.gov (go to the "Workspace" view and click the "View" button under the Incident Report Number) or in fsd.gov (directions on how to do this can be found here). Entities can communicate with an EVS (Entity Validation System) agent in FSD.gov or by responding to the email. If the entity is unable to generate an incident report for some reason (this was a problem we saw this past week), the entity can also go to FSD.gov and start a chat with an agent by clicking on the "live chat" button in the lower right-hand corner. Agents are available from 8AM to 8PM EST.

Once they are contacted by the EVS agent, the entity will have 5 days to respond, or the incident report will be automatically closed and they will have to start again. If the entity needs more time, they should respond to the EVS agent and communicate this. If the ticket is closed, when the entity starts a new one they should include the original ticket number in the Comments Section. Requested documents need to be uploaded at sam.gov, not at fsd.gov. Once the FSD agent has confirmed the entity has been validated, the entity is not done! It will need to go back to SAM.gov to enter its information again and select the current, correct entity info. This step must be done in order to generate the UEID.

Attachment E: RFA Details and Full Legal Terms and Conditions

Responsibility Determination
Digital Frontiers will not enter into a grant agreement with an Applicant prior to ensuring Applicant responsibility. Required documentation includes:

- Evidence of legal documentation or licenses to operate in your country of registration
- Confirmation that products or services used in the performance of the grant are not from a Prohibited Country (explained in Section C)
- Evidence of a Unique Entity ID (UEI) number, CAGE/NCAGE code, and proof of registration with the System for Award Management (SAM) (explained in Annex 5). Evidence of these items are not required to submit an application, but must be provided if selected for a grant award
- Documentation that the Applicant can comply with the award conditions, has a satisfactory record of integrity and business ethics, and has the required financial capacity (explained in Annex 4)

Late Applications
All applications received by the deadline will be reviewed for responsiveness and programmatic merit according to the specifications outlined in these guidelines and the application format. Section C addresses the evaluation procedures for the applications. Applications which are submitted late or are incomplete run the risk of not being considered in the review process.

US Government Registrations
There are mandatory requirements for grantees to obtain the following items/registration before a grant can be awarded. Without registering in the required databases, DAI and LBE cannot deem an Applicant to be “responsible” to conduct business with and therefore, DAI and LBE will not enter into an agreement with any such organization. The award of a grant resulting from this RFA is contingent upon the winner providing a Unique Entity Identifier (UEI) number, a Commercial and Government Entity/NATO Commercial and Government Entity) CAGE/NCAGE code, and proof of registration in the System for Award Management (SAM) system.

Applicants must obtain the following before award:

i. UEI Number
ii. Registration with SAM.gov
iii. CAGE/NCAGE

Instructions for obtaining a UEI number r, SAM registration, or a CAGE/NCAGE are provided in Annex 5.

Prohibited Countries: Prohibited countries are countries that the US Government does not do business with, previously referred to as foreign policy restricted countries. The Applicant may not procure goods or services from the Office of Foreign Assets Control (OFAC) comprehensive sanctioned countries: Cuba, Iran, North Korea, Sudan, and Syria. By submitting an application in response to this RFA, the Applicant certifies that proposed equipment will not be procured from vendors located in one the OFAC prohibited countries above, nor will the origin of any of the parts be from a prohibited country.

Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment – Applicants warrant that all services and products included in their application are compliant with the restrictions contained in 2 CFR 200.216. Grant funds cannot be used to procure or obtain equipment, services, or systems that use covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in Public Law 115-232, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

Full text of this restriction may be accessed here: https://www.ecfr.gov/cgi-bin/text-idx?SID=e3052be29eb6a936bcf083bf38cacd7d&mc=true&node=se2.1.200_1216&rgn=div8

Separate Account: A separate account must be established to house all funds provided under the grant, as well as all interest income.

Permitted Uses of Program Income: The Grantee will inform DAI and LBE of any program income generated under the grant and agrees to follow USAID’s disposition requirements for such program income, which is in accordance with 2 CFR 200 Subpart D. Program income earned under this agreement shall be applied and used in the following descending order:

1. Added to funds committed by USAID and the recipient to the project or program, and used to further eligible project or program objectives;
2. Used to finance the non-Federal share of the project or program; and
3. Deducted from the total project or program allowable cost in determining the net allowable costs on which the federal share of costs is based.

If the terms and conditions of the award do not specify how program income is to be used, then number 2) shall apply automatically. Grantees who are commercial organizations may not apply Option 1) to their program income.

Use of Funds: Funds provided under any grant awarded shall be used exclusively for grant purposes. Diversion of grant funds to other uses will result in cancellation of award and retrieval of funds disbursed to the grant recipient.

Reporting Procedures: A description of reporting requirements will be included in the Grant Agreements.

Project Monitoring: DAI and LBE staff will monitor projects in terms of both programmatic and financial aspects. Grant recipients will be expected to facilitate monitoring by making relevant information available to DAI and LBE staff.

Restrictions: The Grant Funds provided under the terms of this Agreement shall not be used to finance any of the following:

1. Goods or services which are to be used primarily to meet military requirements or to support police or other law enforcement activities,
2. Surveillance equipment,
3. Equipment, research and/or services related to involuntary sterilization or the performance of abortion as a method of family planning,
4. Gambling equipment, supplies for gambling facilities or any hotels, casinos or accommodations in which gambling facilities are or are planned to be located,
5. Activities which significantly degrade national parks or similar protected areas or introduce exotic plants or animals into such areas, or
6. Establishment or development of any export processing zone or designated area where the labor, environmental, tax, tariff, and/or safety laws of the country in which such activity takes place would not apply.
7. Pharmaceuticals,
8. Pesticides,
9. Logging equipment,
10. Luxury goods (including alcoholic beverages and jewelry),
11. Establishing or expanding any enterprise that will export raw materials that are likely to be in surplus in world markets at the time such production becomes effective and that are likely to cause substantial injury to U.S. producers,
12. Activities which would result in the loss of forest lands due to livestock rearing, road construction or maintenance, colonization of forest lands or construction of dams or other water control structures,
13. Activities which are likely to have a significant adverse effect on the environment, including any of the following (to the extent such activities are likely to have a significant adverse impact on the environment):
    - i.) Activities which may lead to degrading the quality or renewability of natural resources;
    - ii.) Activities which may lead to degrading the presence or health of threatened ecosystems or biodiversity;
    - iii.) Activities which may lead to degrading long-term viability of agricultural or forestry production (including through use of pesticides);
    - iv.) Activities which may lead to degrading community and social systems, including potable water supply, land administration, community health and well-being or social harmony.
14. Activities which are likely to involve the loss of jobs in the United States due to the relocation or expansion outside of the United States of an enterprise located in the United States, or
15. Activities which the Grantee is aware are reasonably likely to contribute to the violation of internationally or locally recognized rights of workers,
16. Activities to support the production of agricultural commodities for export from Malawi when such commodities would directly compete with exports of similar United States agricultural commodities to third countries and have a significant impact on United States exporters.

Pursuant to 2 CFR 700.13, it is USAID policy not to award profit under assistance instruments such as grant awards. However, all reasonable, allocable, and allowable expenses, both direct and indirect, which are related to the grant program and are in accordance with applicable cost standards), may be paid under the grant.

For non-US organizations, the Standard Provisions for Non-US Nongovernmental Recipients will apply (http://www.usaid.gov/missions/sa/usaidsa/mandatorystandard.pdf). For US organizations, 2 CFR 200 Subpart D, OMB Circulars (http://www.whitehouse.gov/omb/circulars/a122/a122.html), and the Standard Provisions for U.S. Nongovernmental Recipients will apply.

Cost Application Instructions

- Cost Applications must include:
    - Projected Grant Budget
    - Budget Narrative
    - Completed Financial Capability Questionnaire
    - NICRA or Audited Financial Statements, as available

- Registration of Incorporation Documents
- Personnel, finance, and procurement manuals

Completed Budget. All budget lines must be clearly linked to specific project activities. Supporting information shall be provided, as necessary, in sufficient detail to allow a complete analysis of each line item cost.

Budget Narrative. The budget must have an accompanying budget narrative and justification that provides in detail the estimated costs for implementation of activities listed in the technical application narrative. The combination of the cost data and narrative must be sufficient to allow a determination of whether the costs estimated are reasonable.

Completed Financial Capability Questionnaire, found in Annex 4**,** which includes:

b. **NICRA or** (if no NICRA) **Audited Financial Reports:** Copy of the applicant's most recent financial report, which has been audited by a certified public accountant or other auditor satisfactory to DAI. If no recent audit, a "Balance Sheet" and "Income Statement" for the most current and previous fiscal year.

c. **Incorporation Papers or Certificate of Registration and Statute**

Signing of Grant Agreements

Upon USAID concurrence of the applicant, a Grant Agreement will be prepared. After DAA and the successful applicant have signed the Grant Agreement, all reporting and contractual obligations will be explained to the grant recipients. Section D - Program Description

Certifications, Assurances, Other Statements of the Recipient

In accordance with ADS 303.3.8, DAI will require the winner of this RFA to submit a
signed copy of the following certifications and assurances, **as applicable.**

DAI will provide these certifications to the RFA winner and assist in their completion.

1. Assurance of Compliance with Laws and Regulations Governing Non-Discrimination in Federally Assisted Programs *(Note: This certification applies to Non-U.S. organizations if any part of the program will be undertaken in the United States.)*
2. Certification Regarding Lobbying *(This certification applies to grants greater than $100,000.)*
3. Prohibition on Assistance to Drug Traffickers for Covered Countries and Individuals (ADS 206)
4. Certification Regarding Terrorist Financing, Implementing Executive Order 13224
5. Certification Regarding Trafficking in Persons, Implementing Title XVII of the National Defense Authorization Act for Fiscal Year 2013 *(Note: This certification applies if grant for services required to be performed outside of the United States is greater than $500,000. This certification must be submitted annually to the USAID Agreement Officer during the term of the grant.)*
6. Certification of Recipient

In addition, the following certifications will be included **Part II – Key Individual Certification Narcotics Offenses and Drug Trafficking** *(Note: Only as required per ADS 206 for Key Individuals or Covered Participants in covered countries.)*

Part III – Participant Certification Narcotics Offenses and Drug Trafficking *(Note: Only as required per ADS 206 for Key Individuals or Covered Participants in covered countries.)*

Part IV – Representation by Organization Regarding a Delinquent Tax Liability or a Felony Criminal Conviction
Part V – Other Statements of Recipient
Part VI – Standard Provisions for Solicitations

(Note: Parts V & VI – Are included in the grant file as part of the grant application.)

DAI and USAID reserve the right to fund any or none of the applications received

Attachment F: Grantee Financial Capacity Questionnaire

The main purpose of this questionnaire is to understand the systems adopted by your institution for financial oversight and accounting of grant funds, especially those provided through the U.S. Federal Government. The questionnaire will assist DAI program and accounting staff to identify the extent to which your institution's financial systems match the requirements of the U.S. Federal Government. This information will help the program staff work with you and your institution to review any problem areas that may be identified; thereby avoiding any problems or oversights which would be reportable should an audit of the program or institution be required.

The questionnaire should be completed by the financial officer of your institution in collaboration with DAI program staff. This questionnaire is informational only, and will not have any bearing on the agreement to support your institution based on the technical merit of the application. Therefore, please answer all questions to the best of your knowledge.

While 2 CFR 200 does not cover awards to non-U.S. recipients, DAI shall rely on the standards established in that regulation in determining whether potential non-U.S. recipients are responsible to manage Federal funds. A determination shall be made on the potential recipient's ability, or potential ability, to comply with the following USAID and federal-wide policies:

1) 2 CFR 200 Subpart D (Financial and Program Management);
2) 2 CFR 200 Subpart D (Property Standards);
3) 2 CFR 200 Subpart D (Procurement Standards); and
4) 2 CFR 200 Subpart D (Performance and Financial Monitoring and Reporting).

SECTION A: General Information

Please complete this section which provides general information on your institution.

Name of Institution: ______________________________

Name and Title of Financial Contact Person: ______________________________

Name of Person Filling out Questionnaire: ______________________________

Mailing Address: ______________________________

____

____

Street Address (if different) ______________________________

____

Telephone, Fax, Email (if applicable) ______________________________

Enter the beginning and ending dates of your institution's fiscal year:

From: (Month, Day) ______________ To: (Month, Day) ______________

SECTION B: Internal Controls

Internal controls are procedures which ensure that: 1) financial transactions are approved by an authorized individual and are consistent with U.S. laws, regulations and your institution's policies; 2) assets are maintained safely and controlled; and 3) accounting records are complete, accurate and maintained on a consistent basis. Please complete the following questions concerning your institution's internal controls.

1. Does your institution maintain a record of how much time employees spend on different projects or activities?

Yes: □ No: □

2. If yes, how?

____

____

____

3. Are timesheets kept for each paid employee?

Yes: □ No: □

4. Do you maintain an employment letter or contract which includes the employee’s salary?

Yes: □ No: □

4. Do you maintain inventory records for your institution's equipment?

Yes: □ No: □ (if no, explain)

____

____

____

5. How often do you check actual inventory against inventory records?

____

____

____

6. Are all financial transactions approved by an appropriate official?

Yes: □ No: □

7. The person responsible for approving financial transactions is: ________________ Title: ______________

8. Is the person(s) responsible for approving transactions familiar with U.S. Federal Cost principles as described in OMB Circular A-122?

Yes: □ No: □

9. Does your institution use a payment voucher system or some other procedure for the documentation of approval by an appropriate official?

Yes: □ No: □

10. Does your institution require supporting documentation (such as original receipts) prior to payment for expenditures?

Yes: □ No: □

11. Does your institution require that such documentation be maintained over a period of time?

Yes: □ No: □

If yes, how long are such records kept? ____

12. Are different individuals within your institution responsible for approving, disbursing, and accounting of transactions?

Yes: □ No: □

13. Are the functions of checking the accuracy of your accounts and the daily recording of accounting data performed by different individuals?

Yes: □ No: □

14. Who would be responsible for financial reports? ____

SECTION C: Fund Control and Accounting Systems

Fund Control essentially means that access to bank accounts and/or other cash assets is limited to authorized individuals. Bank balances should be reconciled periodically to the accounting records. If cash cannot be maintained in a bank, it is very important to have strict controls over its maintenance and disbursement.

An Accounting System accurately records all financial transactions, and ensures that these transactions are supported by documentation. Some institutions may have computerized accounting systems while others use a manual system to record each transaction in a ledger. In all cases, the expenditure of funds provided by the USAID-funded program must be properly authorized, used for the intended purpose, and recorded in an organized and consistent manner.

1. Does your institution maintain separate accounting of funds for different projects by:

Separate bank accounts: □

A fund accounting system: □

2. Will any cash from the grant funds be maintained outside a bank (in petty cash funds, etc.)?

Yes: □ No: □

If yes, please explain the amount of funds to be maintained, the purpose and person responsible for safeguarding these funds.

4. If your institution doesn't have a bank account, how do you ensure that cash is maintained safely?

5. Does your institution have written accounting policies and procedures?

Yes: □ No: □

6. How do you allocate costs that are “shared” by different funding sources, such as rent, utilities, etc.?

7. Are your financial reports prepared on a:

Cash basis: □ Accrual basis: □

8. Is your institution's accounting system capable of recording transactions, including date, amount, and description?

Yes: □ No: □

9. Is your institution's accounting system capable of separating the receipts and payments of the grant from the receipts and payments of your institution’s other activities?

Yes: □ No: □

10. Is your institution's accounting system capable of accumulating individual grant transactions according to budget categories in the approved budget?

Yes: □ No: □

10. Is your institution's accounting system designed to detect errors in a timely manner?

Yes: □ No: □

11. How will your institution make sure that budget categories and/or overall budget limits for the grant will not be exceeded?

12. Are reconciliations between bank statements and accounting records performed monthly and reviewed by an appropriate individual?

Yes: □ No: □

13. Briefly describe your institution's system for filing and keeping supporting documentation.

SECTION D: Audit

The grant provisions require recipients to adhere to USAID regulations, including requirements to maintain records for a minimum of three years to make accounting records available for review by appropriate representatives of USAID or DAI, and, in some cases, may require an audit to be performed of your accounting records. Please provide the following information on prior audits of your institution.

1. Is someone in your institution familiar with U.S. government regulations concerning costs which can be charged to U.S. grants (OMB Circular A-122 "Cost Principles for Nonprofit Institutions" and OMB Circular A-110 "Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals and Other Non-Profit Institutions")?

Yes: □ No: □

2. Do you anticipate that your institution will have other sources of U.S. government funds during the period of this grant agreement?

Yes: □ No: □

3. Have external accountants ever performed an audit of your institution's financial statements?

Yes: □ No: □

If yes, please provide a copy of your most recent report.

4. Does your institution have regular audits?

Yes: □ No: □

If yes, who performs the audit and how frequently is it performed?

5. If you do not have a current audit of your financial statements, please provide this office with a copy of the following financial statements, if available:

a. A "Balance Sheet" for the most current and previous year; and
b. An "Income Statement" for the most current and previous year.

6. Are there any circumstances that would prevent your institution from obtaining an audit?

Yes: □ No: □

If yes, please provide details:

____

____

____

CHECKLIST AND SIGNATURE PAGE

DAI requests that your institution submit a number of documents along with this completed questionnaire. Complete this page to ensure that all requested information has been included.

Complete the checklist:
□ Copy of your organization's most recent audit is attached.
□ If no recent audit, a "Balance Sheet" "Income Statement" for the most current and previous fiscal year.
□ All questions have been fully answered.
□ An authorized individual has signed and dated this page.

Optional:
□ Incorporation Papers or Certificate of Registration and Statute is attached.
□ Information describing your institution is attached.
□ Organizational chart, if available is attached (if applicable).

The Financial Capability Questionnaire must be signed and dated by an authorized person who has either completed or reviewed the form.

Approved by:

____

Print Name

____

Signature

____

Title Date ____________