Digital Frontiers - Digital Asia Accelerator
Request for Application (RFA)

RFA No.	2022-16
Issue Date	August 29, 2022
Title	Women's Participation in Southeast Asia's Cybersecurity Sector
Issuing Office & Email	Digital Frontiers c/o DAI DAA_subawards@dai.com
Deadline for Receipt of Questions	September 12, 2022, 5pm EST, to DAA_subawards@dai.com
Deadline for Receipt of Applications	September 28, 5pm EST, to DAA_subawards@dai.com
Point of Contact	DAA_subawards@dai.com
Anticipated Award Type	Fixed Amount Award

The purpose of this Request for Applications (RFA) is to solicit applications for funding. DAI through the United States Agency for International Development (USAID), is seeking an organization to conduct research and write a report on the state of the cybersecurity workforce, the workforce gap, and women's participation in the sector (the gender gap), in five target countries: Cambodia, Indonesia, Laos, Mongolia, and Thailand. The report will also identify challenges to closing the gender gap in those countries and recommendations on how to address the gap.

This research will be done in support of International Telecommunications Union (ITU)'s Women in Cyber (WiC) Mentorship Asia-Pacific (ASP) Programme 2022, and lay the foundations for future iterations of the Programme, through data-driven targeted capacity development

USAID's Digital Asia Accelerator activity ("the Accelerator"), managed by DAI, aims to increase the safe and appropriate use of digital technology for economic development in Southeast Asia. The Accelerator 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.

The Digital Asia Accelerator anticipates issuing an award for an organization for research in five countries: Cambodia, Indonesia, Laos, Mongolia, and Thailand. Applicants should consider budgets in the range of **$80,000 to $100,000** in support of this activity. The expected duration of DAI support or the period of performance is 6 months.

Applications must be received via email to DAA_subawards@dai.com. Any questions concerning this RFA should be submitted in writing to the same email address.

Award will be made to the responsible applicant(s) whose application(s) offers the best value and meets the eligibility requirements.

Issuance of this RFA does not constitute an award commitment on the part of DAI, nor does it commit DAI to pay for costs incurred in the preparation and submission of an application. Further, DAI reserves the right to reject any or all applications received. Applications are submitted at the risk of the applicant. All preparation and submission costs are at the applicant's expense. DAI reserves the right to fund any or none of the applications submitted.

Thank you for your interest in Digital Asia Accelerator activities!

WARNING: Prospective Applicants who have received this document from a source other than the DAA_subawards@dai.com email address, should immediately contact DAA_subawards@dai.com and provide their name and email address in order that amendments to the RFA or other communications can be sent directly to them. Any prospective Applicant who fails to contact DAA_subawards@dai.com assumes complete

responsibility in the event that they do not receive communications prior to the closing date. Any amendments to this RFA, questions and answers, or other communications will be issued from DAA_subawards@dai.com.

Table of Contents

Section A – Grant Application Instructions

A. Completion and submission of applications

Eligibility Requirements

- Applicants must be registered US or non-US organizations regardless of type (for example: for profit, not-for-profit, civic groups and others)
- All Applicants must be willing to forego profit per 2 CFR 700.13
- The following are not eligible:
  - Government entities
  - Individuals
- Applications must be submitted in English, and able to develop project materials in English
- Applications from consortia are welcome.
- Target partner organizations that DAI is searching for include Business networks, chambers of commerce, trade associations, non-governmental organizations (NGOs) focused on digital technology, etc. (national and regional).

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 Identifier (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)

Deadlines

Applications must be received via email to DAA_subawards@dai.com by September 28, 2022, at 5pm EST. Please include the RFA number 2022-16 in the subject line of the email.

Requests for clarification or additional information must be submitted in writing via email to DAA_subawards@dai.com by September 12, 2022 at 5 pm EST. No questions will be answered by phone. Any verbal information received from a DAI or Digital Frontiers employee or other entity shall not be considered as an official response to any question regarding this RFA. Copies of questions and responses will be distributed via email to all prospective applicants who are on record as having received this RFA after the submission date specified in the Synopsis above.

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.

B. Preparation Instructions – Technical Application

A complete RFA application consists of the following sections:

- Narrative technical application (15 pages maximum)
- Completed Project Workplan
- CVs of all named project team members. CVs should be no longer than 3 pages each

Page Limitation: Applications should be specific, complete, presented concisely and shall not exceed **15 pages** (exclusive of personnel CVs and proposed workplan) in Word format.

Technical application requirements

Applicants are invited to submit applications that address the objectives and outcomes contained in Section D. Program Description and the evaluation criteria on page [9].

Applications must include the following components:

- **Narrative technical approach** outlining how the applicant would execute the duties and responsibilities outlined below. A **project workplan** should be included with approximate timelines and key milestones.

- **Staffing plan** outlining the staff who will work on this project and a description of their roles and responsibilities. Applicants should include short bios for the top three team members (1-page bio maximum for each team member).

- **Previous experience** Summary descriptions of at least three of the applicant's relevant past projects. Applicants must demonstrate relevant working experience in at least one of the Accelerator's countries and include summary descriptions of three relevant projects that demonstrate the core capabilities required to execute the proposed project, such as project management in multiple countries, survey design, in-depth interviews, and general understanding of the labor markets and cybersecurity.

Applicants must ensure that their applications are received in their entirety. The Digital Asia Accelerator bears no responsibility for data errors resulting from transmission or conversion processes associated with electronic submissions.

C. Preparation Instructions – Cost Application

➢ Cost Applications must include:
- Projected Grant Budget (Annex 3)
- Budget Narrative (Annex 3)
- Completed Financial Capability Questionnaire (Annex 4)
- NICRA or Audited Financial Statements
- Registration of Incorporation Documents
- Personnel, finance, and procurement manuals

1. **Completed Budget.** All budget lines must be clearly linked to specific project activities. See attached Annex 3 for the budget template. Supporting information shall be provided, as necessary, in sufficient detail to allow a complete analysis of each line item cost.

2. **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. A budget narrative template is included in Annex 3.

3. **Completed Financial Capability Questionnaire,** found in Annex 4, which includes:
   a. **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.
   b. **Incorporation Papers or Certificate of Registration and Statute**

Section B - Selection Process

All applications that meet the application requirements will be reviewed by the review panel.

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**.

DAI 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 DAI. DAI 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. DAI 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, DAI may reject an application with the highest technical evaluation in favor of a favorably priced offer. DAI strongly recommends 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:

Evaluation Criteria	Evaluation Sub-criteria	Maximum Points
Narrative Technical Approach	• Proposal demonstrates how they will contribute to the outlined objectives. • Technical approach is implementable within proposed timeframe and resources.	40 points
Staffing Plan	• Personnel plan demonstrates the skills needed to achieve project outcomes.	30 points
Previous Experience	• Proposal includes summary descriptions of at least three of the offeror's relevant past projects that demonstrate the core capabilities required to execute the proposed project, such as project management in multiple countries, survey design, in-depth interviews, and general understanding of the labor markets and cybersecurity.	30 points
Total Points		100 points

Section C - Special Grant Requirements

The applicant shall bear in mind the following special requirements for any grants awarded in response to this RFA:

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 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 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, 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 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 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 staff.

Restrictions: The Grant Funds provided under the terms of this Agreement shall <u>not</u> 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):

<li value="1" style="list-style-type: none;">
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 <u>production</u> 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. 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. Please see Annex 1 for Standard Provisions.

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

---

Signing of Grant Agreements

Upon USAID concurrence of the applicant, a Grant Agreement will be prepared. After DAI 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

D. Program Description

Digital Asia Accelerator

Women's Participation in Southeast Asia's Cybersecurity Sector

Objective

DAI is searching for an organization to conduct research and write a report on the state of the cybersecurity workforce, the workforce gap, and women's participation in the sector (the gender gap), in five target countries: Cambodia, Indonesia, Laos, Mongolia and Thailand. The report will also identify challenges to closing the gender gap in those countries, and recommendations on how to address the gap.

This research will be done in support of International Telecommunications Union (ITU)'s Women in Cyber (WiC) Mentorship Asia-Pacific (ASP) Programme 2022, and lay the foundations for future iterations of the Programme, through data-driven targeted capacity development.

Work Location

This work will be conducted remotely.

Expected Timeline

Projects will run for a maximum of 6 months, starting in October or November 2022.

Background

DIGITAL ASIA ACCELERATOR
I.   Digital Asia Accelerator

USAID's Digital Asia Accelerator project ("the Accelerator"), managed by DAI, aims to increase the safe and appropriate use of digital technology for economic development in Southeast Asia and Mongolia. The Accelerator 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.

The Accelerator's objectives are to:

1. Increase **public awareness of digital safety** issues to increase safe behavior online;
2. Improve **digital skills** of the private sector and civil society; and
3. Strengthen the ability of the private sector and civil society to engage on a range of digital economy and cybersecurity **policy issues**.

II.   International Telecommunications Union Efforts to Support Women in Cybersecurity

The first edition of Women in Cybersecurity (WiC) was organised following the October 2020 Global CyberDrill, where a webinar on Empowering Women in Cybersecurity highlighted how there was not only a global workforce shortage in cybersecurity, but also a significant gender gap. The main outcome of the discussions was that while education and training can help women enter the field of cybersecurity, there is value in receiving guidance from other women, being inspired by role models and mentors that can help junior women professionals navigate this male-dominated field and thrive in it.

Following this idea, the pilot edition of the Women in Cyber (WiC) Mentorship Programme was designed to close the cybersecurity workforce and gender gap. The programme was launched on 8th March 2021 to commemorate International Women's Day. It was jointly organized by the ITU Telecommunication Development Sector (ITU-D) and the Forum of Incident Response and Security Teams (FIRST) with the support of EQUALS, the global partnership for gender equality in the digital age of which ITU is a co-founder.

WiC 2021 was first organized focusing on the Arab States and Africa regions. The series was built on three Pillars: 1) Inspire, 2) Train and 3) Empower. Twenty mentors participated, along with 70 mentees (from 12 countries in Africa and 7 Arab States).

III.   2022 WiC Asia-Pacific Program

The WiC programme will be implemented in the Asia Pacific region from April to September 2022, with a group of 50 selected mentees and 14 mentors from the region The Programme is jointly organized with the Forum of Incident Response and Security Teams (FIRST) and EQUALS, the global partnership for gender equality in the digital age, co-founded by ITU. It is grounded on the same three pillars of WiC 2021:

Pillar 1: Inspire

This first pillar includes a selection of Four Inspirational Keynote Webinars, spotlighting high-level female guest speakers from around the world that have led stellar careers in cybersecurity. The INSPIRE series aims to feature well-known women in cybersecurity who have achieved successful careers in the field. The series would promote role models, and inspire young women professionals to consider cybersecurity as a valid option for a fulfilling career.

Pillar 2: Train

The training will include various relevant and emergent topics in the cybersecurity field. This would allow Mentees to learn and cultivate a multi-faceted set of skills needed to succeed in cybersecurity. The idea behind the Train pillar is to provide introductory training session on technical trends in cybersecurity. This would touch upon different sectors in the field while also facilitating personal development through soft skills training.

Pillar 3: Empower

This third Pillar pertains to the most pivotal part of the Programme. Through a meticulous matching of Mentees with Mentors based on backgrounds, fields of expertise and wished takeaways from the programme, groups of 2-3 Mentees are matched with each Mentor (also fostering peer-to-peer exchange and community-building).

The Mentorship Circles are spaces where Mentees and mentors are guided in their journey, and can exchange with other participants, before going into private 45-minute Breakout Rooms for each mentoring group. The activities of the mentorship circles include:

1. SMART Goal Setting and Complementary Plan (Documents provided by coordinators include a Session Record and a SMART Goal Sheet);
2. Roles and Responsibilities of Participants (Mentors and Mentees);
3. Follow-Ups on events, trainings, deadlines and actions;
4. Discussion of challenges or hurdles they may have been facing while achieving their set goals; and
5. Skills accumulated through WiC Trainings and/or other sources.

WiC Research

This pilot research will support ITU's WIC Asia Pacific programme. WiC 2021 highlighted the need to identify, research and pinpoint main challenges and gaps for women in the cybersecurity field at the global and regional levels, as the data available is not exhaustive, especially in identifying region-specific challenges.

In support of that, this project will develop initial research outputs on the state of the cybersecurity workforce in Cambodia, Indonesia, Laos, Mongolia and Thailand, the workforce gap[1], and within that focus on the gender gap. It will identify key barriers women face that driving the gender gap, and recommendations for how to address it. The report will be used to support data-driven targeted action to promote and mainstream gender inclusion in cybersecurity, and develop informed, longer-term training and capacity-building frameworks for women in cybersecurity.

DUTIES AND RESPONSIBILITIES
In order to do this, the organization will provide the following outputs:

---

[1] 1.42 million unfilled jobs in the Asia Pacific region, according to ISC2

1. Methodology Assessing the State of the Female Cybersecurity Workforce

Design a methodology to understand the state of the female cybersecurity workforce and how to encourage young women to enter and succeed in the cybersecurity industry. This should include a survey of cybersecurity professionals (including technical, policy/regulatory, academia, and private sector actors), in-depth interviews with cybersecurity professionals to understand their experience, and a catalogue of existing cybersecurity training available. The organization should also consider the methodology and results from the global ISC2 Cybersecurity Workforce Study[2], and the methodology from ITU's 2021 study in Viet Nam[3] in their methodology design. The organization will align with USAID, ITU and DAI on the methodology before deploying it.

Key questions that this research should answer for the five focus countries are:

1) What are the trends related to the cybersecurity workforce gap in the region? What are some region-specific challenges that the cybersecurity field is facing?
2) To what extent are women participating in the cybersecurity workforce? What is the proportion of women in CIRT/CERT/CSIRT?
3) What are the challenges and key barriers that current female cybersecurity professionals see in advancing in the cybersecurity field, or for girls and women looking to enter the cybersecurity field?
4) What efforts are being made to increase diversity in the cybersecurity workforce? For example:
    o What is the current state of cybersecurity capacity development, including with a specific focus on female professionals in the sector?
    o What are the specific incentives/awareness raising efforts for young women to pursue ICT and/or cybersecurity studies, including for female cybersecurity entrepreneurship?
    o Do private sector companies and/or government agencies have specific diversity and inclusion policies in place to attract more women into the cybersecurity workforce?
5) What are the key recommendations on how to encourage more women to have careers in cybersecurity, from entering the sector, through retaining female talent, and advancing careers / reaching senior positions?
6) What are some potential pilot projects/activities in line the questions above?

2. Deployment of Methodology in Five Target Countries.

IV.   Once methodology is approved by ITU, USAID, and DAI, the organization will deploy the methodology in the five target countries. The online survey will be conducted both in English and the local language (Bahasa Indonesia, Laotian, Thai, Mongolian, Khmer) and will be translated by the organization.

The organization should specify the minimum number of participants and/or respondents for the research.

Additionally, the organization will conduct research in both English and the local language on the current state of cybersecurity capacity building programmes in each target country. Additionally, the survey will also be open to respondents in general from Asia-Pacific in English.

During this phase, ITU, USAID, and DAI will assist with outreach and disseminating the survey to respondents, including through requesting assistance from the respective United Nations Country Teams.

3. Final Report

The final report will include:

1. The general state of the cybersecurity workforce in the 5 focus countries
2. The cybersecurity workforce gap in the 5 focus countries and specifically regarding women's participation in the sector, including:
    A. Entering the workforce
    B. Talent retention
    C. Career advancement
3. Challenges driving the gender gap
4. Recommendations for addressing these challenges

---

[2] https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38
[3] https://www.itu.int/hub/publication/d-phcb-cyb_educ-vtn-2021/

5. Annexes: Country Profiles for each of the 5 focus countries

Annex 1: Mandatory Standard Provisions

Mandatory Standard Provisions for Non-US Nongovernmental Recipients:
(http://www.usaid.gov/missions/sa/usaidsa/mandatorystandard.pdf)

Annex 2: Certifications, Assurances, Other Statements of the Recipient

In accordance with ADS 303.3.8, DAI will require successful grant applicants to submit a
signed copy of the following certifications and assurances, <u>as applicable:</u>

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: <u>Only as required per ADS 206 for Key Individuals or Covered Participants in covered countries</u>.)*

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

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.)

Annex 3: Sample Budget and Budget Narrative

	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

<u>Budget Narrative Template</u>

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.

Annex 4: Financial Capability Questionnaire

Accounting System and Financial Capability Questionnaire
For DAI Grant Recipients

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 _____

Annex 5: Instructions for Obtaining CAGE/NCAGE Code, SAM Registration, and UEI Number

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.

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

System for Award Management (SAM) Registration
You must have an active registration with www.SAM.govto do business with the Federal Government. To register in SAM, at a minimum, you will need the following information:

      o U.S. Registrants:
      1)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
      2)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)
      o International Registrants:
      1)Your NATO Commercial and Government Entity (NCAGE) Code
      2)Your Legal Business Name and Physical Address from your D&B record.
      o Follow this link to create a SAM.gov user account and register your organization:
https://sam.gov/content/entity-registration

Unique Entity ID (UEI)
By April 4, 2022, the federal government will transition 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.

If your organization already have an active or expired registration: You already have a Unique Entity ID (SAM) and do not need to take action. Learn how to view your Unique Entity ID (SAM). If your renewal is upcoming, use the normal process to renew your entity.

Annex 6: Past Performance Matrix

#	Project Title	Client Name	Brief Description	Contact Name, Phone and Email	Cost in USD$	Start-End Dates
1						
2						
3						
4						
5						

Annex 7: Application Checklist

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

- [ ] Narrative Technical Application
- [ ] Cover Letter
- [ ] CVs of named team members (maximum 3 pages each)
- [ ] Past Project Examples (Annex 6)
- [ ] Workplan
- [ ] Budget
- [ ] Budget narrative
- [ ] Completed Financial Capability Questionnaire
- [ ] NICRA or Audited Financial Reports
- [ ] Incorporation Papers or Certificate of Registration and Statute
- [ ] Personnel, procurement, and finance manuals